

2014-06

# Homeland Security Affairs Journal, Volume X - January-July 2014

Monterey, California. Naval Postgraduate School

Homeland Security Affairs Journal, Volume X - June 2014
http://hdl.handle.net/10945/50322

# HOMELAND SECURITY AFFAIRS

Volume 10
2014

THE JOURNAL OF THE NAVAL POSTGRADUATE SCHOOL
CENTER FOR HOMELAND DEFENSE AND SECURITY

http://www.hsaj.org

# Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model

Richard White

## ABSTRACT

*The 2013 National Infrastructure Protection Plan represents the latest attempt to rectify a faltering program that has suffered from the absence of a viable risk measure. This article introduces an Asset Vulnerability Model (AVM) to overcome recognized challenges and provide strategic direction in the form of (1) baseline analysis, (2) cost-benefit analysis, and (3) decision support tools. AVM is predicated on Θ, an attacker's probability of failure based on research in game theory. The Θ risk formulation provides a unifying structure within the Department of Homeland Security by combining elements from the Risk Management Framework and National Preparedness System. But critical infrastructure is not the only means of domestic catastrophic attack. Thus this article also proposes a policy framework supported by game theory to extend AVM protection to chemical, biological, radiological, and nuclear stockpiles. In this manner, AVM may account for protective investments and lead the nation towards a unified homeland security strategy.*

## INTRODUCTION

The attacks of September 11, 2001, exposed the vulnerability of critical infrastructure to precipitating domestic catastrophic attack through asymmetric means. In the intervening decade, the Department of Homeland Security (DHS) has struggled to develop a coherent infrastructure protection program. Various reviews reveal a program that is fragmented, uncoordinated, and adrift. The central difficulty has been in developing a risk assessment formulation to adequately inform strategic investment decisions. Without an appropriate measure, DHS is unable to (1) assess current protective status, (2) evaluate future protective improvement measures, or (3) justify national investments.

This paper examines current DHS infrastructure protection programs and the underlying challenges to developing an adequate risk assessment formulation. It then addresses these challenges before introducing an Asset Vulnerability Model (AVM) to overcome them and help provide strategic direction. It draws on insight from earlier research in game theory suggesting a coordinated defense for both critical infrastructure and domestic stockpiles of chemical, biological, radiological, and nuclear (CBRN) agents. It concludes by proposing a policy framework supporting interagency coordination protecting both sets of assets under a unified homeland security strategy.

## CRITICAL INFRASTRUCTURE PROTECTION

On September 11, 2001, elements of the aviation infrastructure were exploited to attack the World Trade Center and the Pentagon representing seats of US economic and military power (The White House 2003, 8).[1] Nearly 3,000 people were killed and $41.5 billion suffered in damages.[2] 9/11 was a "wake-up call" to the catastrophic potential of critical infrastructure (The White House 2003, 5).[3] As a result, the 2002 Homeland Security Act made critical infrastructure protection a core mission of the newly created Department of Homeland Security.[4] Today, the 2013 *National Infrastructure Protection Plan* (NIPP) guides this mission. At the heart of the plan is the Risk Management Framework (RMF), a five-step process for identifying, prioritizing, applying, and evaluating infrastructure protection improvement measures.[5] A 2010 review by the National Research Council (NRC) determined that "DHS's operationalization of

that framework—its assessment of individual components of risk and their integration into a measure of risk—is in many cases seriously deficient and is need of major revision."[6] Various other reviews support the NRC's findings.

Starting with Step Two, "Identify Infrastructure," the DHS Inspector General (IG) concluded that the National Asset Database contained "many unusual or out-of-place assets whose criticality is not readily apparent, and too few assets in essential areas and may represent an incomplete picture." The assets in question included 4,055 malls, shopping centers, and retail outlets, 224 racetracks, 539 theme parks and 163 water parks, 1,305 casinos, 234 retail stores, 514 religious meeting places, 127 gas stations, 130 libraries, 4,164 educational facilities, 217 railroad bridges, and 335 petroleum pipelines. Notably missing from the database were many other items from banking and finance and food and agriculture sectors.[7]

In Step Three, "Assess and Analyze Risks", the Government Accountability Office (GAO) found that less than 11 percent of DHS' assessments were conducted on high-priority assets. According to the GAO, DHS conducted about 2,800 combined surveys over a two-year period from 2009 to 2011. Of these, GAO was able to identify 179 assessments conducted on high-priority assets. Because of discrepancies between lists, GAO acknowledged another 129 assessments might also have been done on high priority assets.[8] GAO acknowledged that DHS had little control over industry participation in the voluntary program, but also noted that DHS (1) had not developed institutional performance goals to measure owner/operator participation, nor (2) positioned itself to assess why some high-priority asset owners and operators declined to participate.[9]

Moreover, the Homeland Security Grant Program (HSGP) raised a furor in 2006 when Wyoming received $28.34 per capita compared to $4.10 and $3.73 per capita for New York and California respectively. After the 9/11 Commission weighed in on the issue, and spurred by Congressional legislation, DHS undertook to develop a more risk-based approach for determining HSGP allocations. Accordingly, the 2007 HSGP grant guidance announced the adoption of the risk formula R=T*V*C where T is the likelihood of an attack occurring, V is the vulnerability to an attack, and C is the potential consequences of an attack. In applying the formula, however, DHS was unable to differentiate vulnerability across areas and states, and consequently assigned it a constant value of one.[10] In effect, DHS treated all assets as equally vulnerable to make resource decisions about reducing vulnerability.

In Step Four, "Implement Risk Management Activities," a 2011 Congressional Research Service (CRS) report indicated a lack of coordination between the RMF working "inside the perimeter" of critical infrastructure, and the National Preparedness System working "outside the perimeter" of critical infrastructure. According to the CRS report,

> It is not clear to what extent the NIPP process influences the allocation of resources to states and localities. DHS states that information contained in its list of high-priority sites is reviewed when making these grant allocation decisions. However, these grants are managed by FEMA, which apparently assesses risk independent of the NIPP.[11]

Between 2001 and 2008, DHS gave approximately $12 billion to state and local governments to prepare for and respond to terrorist attacks and other disasters.

> A central question that may be asked is what has been the rate of return, as defined by identifiable and empirical risk reductions, on this $12 billion investment? It does not appear, however, that there is an established methodology to engage in such analyses, nor are the data sets necessary for such analyses well-developed.[12]

Indeed, the National Research Council

> [D]id not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making… Moreover, it is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses other than for natural disasters.[13]

Developing an appropriate risk measure is essential to guiding homeland security strategy, without which it is impossible to (1) assess current status, (2) evaluate future measures, or (3) justify national investments. Furthermore, it is a requirement under the 1993 Government Performance and Results Act. That the 2014 DHS budget justification to Congress does not include such measures for infrastructure protection indicates this is still a pertinent issue.[14] The state of affairs is of such a concern that in February 2013 the Obama Administration issued Presidential Policy Directive 21 calling for a review and analysis of current efforts to advance "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[15]

## RISK ASSESSMENT CHALLENGES

Among its conclusions, the National Research Council found that the DHS Risk Management Framework "is sound and in accord with accepted practice in the risk analysis field."[16] Risk management is "a continual process or cycle in which risks are identified, measured, and evaluated; countermeasures are then designed, implemented and monitored to see how they perform, with a continual feedback loop for decision-makers input to improve countermeasures and consider tradeoffs between risk acceptance and avoidance."[17] Where the NRC took exception was with the DHS risk assessment formulation R=f(T,V,C).[18]

Risk assessment "pertains to the quantification or measurement of identified risk and probabilistic assessment that certain risks will manifest themselves."[19] By one estimate, there are more than 250 proposed risk assessment methodologies for critical infrastructure alone.[20] Ted Lewis wrote the textbook on risk analysis for critical infrastructure protection.[21] Lewis applies a threat-driven approach to risk assessment. Threat-driven methodologies begin with a predefined set of initiating events. A 2001 study indicated that 80 percent of risk assessment models are of the event- or threat-driven variety.[22] Threat-driven approaches are supported by decades of experience in safety and reliability engineering using logic trees, influence diagrams, causal loop diagrams, and other methods to model human-initiated events.[23] According to McGill, "threat-driven approaches are appropriate for studying initiating events that are well understood and whose rate of occurrence can be reliably predicted from historical data; however, they ultimately fail to consider emerging or unrecognized threats devised by an innovative adversary...."[24] In the insurance or financial sectors, the assessment of risk benefits from a rich and voluminous set of data which can be mined for patterns of historical behavior. While there are various governmental and non-governmental databases on terrorism, these data sources are relatively less robust.[25] The National Research Council concurs that "with respect to exceedingly rare or never-observed events, the historical record is essentially nonexistent, and there is poor understanding of the sociological forces from which to develop assessment techniques." They concluded: "Thus, it will rarely be possible to develop statistically valid estimates of attack frequencies (threat) or success probabilities (vulnerability) based on historical data."[26]

Altogether the 2010 National Research Council report cited ten challenges to developing a risk formulation adequate for guiding strategic investment decisions.[27] In addition to the difficulty of making reliable threat predictions, the NRC cautioned against risk formulations that were either too simple or too complex. The problem with developing high fidelity risk models is the same lack of historical data that troubles threat estimation. In the absence of hard data, assumptions must be made. The more complex the model, the more assumptions must be made, compounding potential errors. The middle ground, recommended by the NRC, is to develop risk models that are "documented, transparent, and repeatable."[28] For the purpose of guiding strategic decisions, the risk formulation must also be comprehensive in scope. According to the NRC report, "vulnerability is much more than physical security; it is a complete systems process consisting at least of exposure, coping capability, and longer term accommodation or adaptation."[29] In other words, the risk

formulation should address all phases of disaster, currently identified in the FEMA Integrated Emergency Management System as prevent, protect, mitigate, respond, and recover.[30] Similarly, the risk formulation needs to capture the broader effects of a disaster beyond the immediate damage. "DHS's consequence analyses tend to limit themselves to death, physical damage, first-order economic effects, and in some cases, injuries and illness."[31] Ultimately, the effectiveness of any risk formulation is judged by its usefulness to decision makers in managing resources. According to the National Research Council, the attributes of a good risk analysis include the ability to (1) convey current risk levels, (2) support cost-benefit analysis, (3) demonstrate risk reduction effects across multiple assets at different levels of management, and (4) measure and track investments and improvement in overall system resiliency over time.[32]

The preceding summary does not address all the challenges identified by the National Research Council, but provides sufficient criteria for making a cursory evaluation of some current risk models. A 2006 survey identified thirty critical infrastructure models specializing in interdependency analysis.[33] A separate survey in 2012 identified twenty-one critical infrastructure risk models for informing strategic decisions.[34] Together, the two surveys identified forty-one distinct models. McGill's Critical Asset and Portfolio Risk Analysis (CAPRA) was also added, making a total of forty-two models (See Table 1). The limited information available was sufficient to examine only the twenty-two models identified in bold text in Table 1. Of the twenty-two models examined, twelve used a threat-driven approach, seven were described as "complicated," fourteen did not address "resiliency", and two did not capture the broader impacts of a disaster. None of the models appeared to satisfy the NRC challenges.

**Table 1:** Critical Infrastructure Risk Assessment Models

| | |
|---|---|
| 1. AIMS | 22. IIM |
| 2. Athena | 23. KM&V |
| 3. BIRR | 24. MDM |
| 4. BMI | 25. MIN |
| 5. CAPRA | 26. MUNICIPAL |
| 6. CARVER2™ | 27. N-ABLE |
| 7. CIMS | 28. NEMO |
| 8. CIP | 29. Net-Centric GIS |
| 9. CIPDSS | 30. NEXUS-FF |
| 10. CIPMA | 31. NGtools |
| 11. CISIA | 32. NSRAM |
| 12. CommAspen | 33. PFNAM |
| 13. COUNTERACT | 34. RAMCAP-Plus |
| 14. DECRIS | 35. RMCIS |
| 15. DEW | 36. RMF (DHS) |
| 16. EMCAs | 37. RVA |
| 17. EURACOM | 38. SRAM |
| 18. FAIT | 39. TRAGIS |
| 19. FINSIM | 40. TRANSIMS |
| 20. Fort Future | 41. UIS |
| 21. IEISS | 42. WISE |

## SHAPING AN ADEQUATE RISK FORMULATION

Obviously, an adequate risk formulation for guiding strategic decisions needs to overcome the previous challenges. The foremost challenge is overcoming the inherent problems to the threat-driven approach. Adopting an asset-driven approach may do this. An asset-driven approach estimates the consequences and probability of adversary success for an exhaustive set of plausible initiating events without regard to their probability of occurrence, and then overlays their likeliness of occurrence if such information is available.[35] The main criticism of the asset-driven approach is that it is an "impact analysis" not a "risk analysis."[36] Without a firm probability occurrence, the asset-driven approach is deemed less efficient at allocating resources where they're most needed; i.e., the assets most likely to be attacked. Again, the dearth of attack data renders robust statistical analysis problematic. By comparison,

natural hazards have amassed a great deal of data and been subject to extensive statistical analysis. Even with this advantage, forecasters still can't predict with certitude where or when a natural disaster will strike. The primary benefit of statistical analysis to hazard prediction is in localizing their effects. Thus, for example, while earthquakes are a national phenomenon, California justifiably bears the cost of more stringent seismic standards compared to Connecticut. Localization can be similarly applied to critical infrastructure without the benefit of statistical analysis. Homeland Security Presidential Directive 7 does this by specifying protection for critical infrastructure "whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to the use of a weapon of mass destruction… [or] have a debilitating effect on security and economic well-being."[37] Of the sixteen infrastructure sectors currently categorized by the federal government, the nine listed in Table 2 could be targeted to precipitate mass or debilitating effects.

**Table 2:** Critical Infrastructure Threats

| |
|---|
| 1. Chemical Plants |
| 2. Dams |
| 3. Energy |
| 4. Financial Services |
| 5. Food & Agriculture |
| 6. Information Networks |
| 7. Nuclear Reactors, Materials, & Waste |
| 8. Transportation Systems |
| 9. Water & Wastewater Systems |

Not included in the list in Table 2 are commercial facilities, communications, critical manufacturing, defense industrial base, emergency services, government facilities, and healthcare and public health. Commercial facilities include 460 skyscrapers, the loss of two of which proved particularly deadly on 9/11. But the collapse of the Twin Towers was due to subversion of the transportation sector turning passenger jets into guided missiles. The buildings themselves did not pose a catastrophic threat and had withstood a conventional bombing attack in 1993. The criticality of large buildings rests in their value as secondary targets where large numbers of people congregate. By themselves, they cannot precipitate mass effects. Similar arguments may be made for the remaining sectors.

Insofar as developing an adequate risk formulation is concerned, it is also important to choose the right metric. An appropriate metric must answer three questions: (1) What is the risk to? (2) What is the risk from? and (3) How much risk is acceptable?[38] To answer these questions, it is necessary to turn to earlier work in game theory.

Game theory is the study of multi-agent decision problems. Most of the current research and applications are conducted by micro-economists, though game theory has also been successfully applied to areas as diverse as computer science and evolutionary biology.[39] Thus, it was not unexpected that game theory should yield valuable insights when it started to be applied to the problem of terrorism in the 1970s.[40] In 1988, Todd Sandler and Harvey Lapan used game theory to examine the strategic relationship between terrorists' choice of targets and the targets' investment decisions. They discovered that an investment decision by one target had a direct impact on the vulnerability or likelihood of attack on the other. From this insight they concluded that (1) a coordinated defense policy among all targets is more efficient than an uncoordinated one, and (2) the optimum defense strategy is to protect all targets equally, not necessarily maximally. Sandler and Lapan's findings were dependent on a particular value representing the terrorist's probability of attack failure, which they designated as $\theta$.[41] Sandler and Lapan's research suggest a metric based on $\theta$ as it answers the three questions: (1) What is the risk to? The risk is to critical infrastructure assets; (2) What is the risk from? The risk is from an attacker; (3) How much risk is acceptable? Targets are optimally protected when they are equally protected.

## AN ASSET VULNERABILITY MODEL

An Asset Vulnerability Model is now introduced to work with the DHS Risk Management Framework and (1) convey current risk levels, (2) support cost-benefit analysis, (3) demonstrate risk reduction effects across multiple assets at different levels of management, and (4) measure and track investments and improvement in overall system resiliency over time. AVM analysis is predicated on a risk measure designated as Θ representing an attacker's probability of failure based on the Sandler and Lapan value θ. The two values differ in that the Sandler and Lapan θ represents an attacker's perception while the AVM Θ represents the defender's known understanding. AVM is comprised of three elements: (1) baseline analysis, (2) cost-benefit analysis, and (3) decision support tools.

Baseline analysis produces a risk profile of all critical assets based on Θ. Theta is calculated in an asset-based risk formula addressing the five phases of emergency management. A separate Θ is calculated for every critical infrastructure asset as listed in Table 2 that may be exploited or destroyed to create mass or debilitating effects. The proposed risk formulation for Θ is as follows:

$$\Theta = P(dis)*P(def)*P(den)*P(dim)*\%dam) \quad (1.0)$$

where

$$P(dis) = \text{Probability an attack can be detected/disrupted} \quad (1.1)$$

$$P(def) = \text{Probability an attack can be defeated} \quad (1.2)$$

$$P(den) = \text{Probability a worst case disaster can be averted} \quad (1.3)$$

$$P(dim) = \text{Probability 100\% of the survivors can be saved} \quad (1.4)$$

$$\%(dam) = \text{\% decrease in economic output * \% increase in mortality rate} \quad (1.5)$$

P(dis) corresponds to the "prevent" phase of emergency management and is calculated from known intelligence data by dividing the number of thwarted attacks by the number of planned and executed attacks. This estimation for stopping an attack is fundamentally different from trying to predict the start of one, making acceptable use of what limited historical data available. P(def) corresponds to the "protect" phase of emergency management. P(def) is derived from the Protective Measure Index (PMI) assessed by security surveys and vulnerability assessments currently conducted by DHS. PMI are assessed at Argonne National Laboratory from data collected by a cadre of DHS Protective Security Advisors, helping maintain consistency of results.[42] P(den) corresponds to the "mitigate" phase of emergency management and examines failure modes and redundancy designed to prevent an asset's incapacitation or subversion. As part of its PMI calculation, Argonne National Laboratory also produces a Resiliency Index that may be used in this estimation.[43] P(dim) corresponds to the "response" phase of emergency management. P(dim) is calculated based on the capacity of first responders to rescue and treat survivors within seventy-two-hours of a catastrophe. A default value may be calculated from historical data for similar size incidents independent of cause. The %(dam) parameter simultaneously represents the "recovery" phase of emergency management and the magnitude component of the risk assessment formula. It taps existing national economic and mortality data capturing the broader impacts for incidents of both mass destruction and disruption.

Cost-benefit analysis finds the optimum combination of security improvement measures proposed for each asset. Cost-benefit analysis is conducted using ΔΘ and D(ΔΘ) for each improvement measure. Delta theta is the estimated increase in Θ for the proposed improvement measure. Delta theta is provided in component form as P(Δdis), P(Δdef), P(Δden), and P(Δdim). The magnitude component, %(dam) remains unchanged as it represents the worst-case disaster if an asset is compromised. An associated cost component is provided for each ΔΘ in the form of D(Δdis),

D(Δdef), D(Δden), and D(Δdim). Each proposed improvement measure has an associated set of paired ΔΘ and D(ΔΘ) data tuples. P(Δdef) and P(Δden) are directly related to assets, whereas P(Δdis) and P(Δdim) represent national and regional improvement measures that are proportionally assigned to affected assets. The given ΔΘ and D(ΔΘ) values are discrete, representing specific capabilities for purchase. The choice of whether or not to buy them is also discrete; there are no fractional solutions. The data sets associated with each improvement are also independent. This stipulation eliminates dependency analysis. Estimating ΔΘ will be difficult enough using either expert elicitation or computer modeling. Consistency will be key, suggesting that ΔΘ should be estimated by a central source, perhaps at Argonne National Laboratory using techniques already developed for the Protective Measure Index and Resilience Index. Cost-benefit analysis calculates the combined ΔΘ and D(ΔΘ) for each asset according to the formulations shown in 2.0 and 3.0. A proportional value is then derived by dividing ΔΘ by D(ΔΘ). The cost-benefit analysis program selects the combination of measures producing the highest proportional value for the given asset.

$$\Delta\Theta = P(\Delta dis)*P(\Delta def)*P(\Delta den)*P(\Delta dim)*\%(dam) \quad (2.0)$$

$$D(\Delta\Theta) = D(\Delta dis)+D(\Delta def)+D(\Delta den)+D(\Delta dim) \quad (3.0)$$

Decision support tools graphically portray the results of baseline and cost-benefit analyses and facilitate various views to present the information in a manner most meaningful to a decision maker. Figure 1.1 portrays the unfiltered results from baseline analysis using simulated data. Real data was unavailable as it is protected under the 2002 Homeland Security Act from disclosure even under the Freedom of Information Act. Alternative views of the data may be selected. For example, Figure 1.2 shows the baseline data sorted by Θ, identifying the most protected to the least protected assets. Figure 1.3 sorts baseline data by asset type, depicting the relative protection of assets within the same sector. Figure 1.4 indicates relative protection of assets within a given geographic region. Other views may also be generated as desired. Similarly, the results from cost-benefit analysis can be graphically portrayed to assist decision makers with allocating resources. For example, Figure 2.1 shows assets ordered by largest to smallest improvement gains, facilitating the purchase of the highest protection within a fixed budget. Figure 2.2 shows assets ordered by improvement cost, facilitating the purchase of the most protection measures within a fixed budget. If the decision maker wishes to concentrate on protecting a particular sector, then improvements can be sorted by asset type as in Figure 2.3. If the decision maker wishes to concentrate on protecting a particular region, then improvements can be sorted by asset location as in Figure 2.4. The significance of these tools is that they provide a snapshot of the current homeland security profile and can inform resource allocation decisions based on any number of different investment strategies.

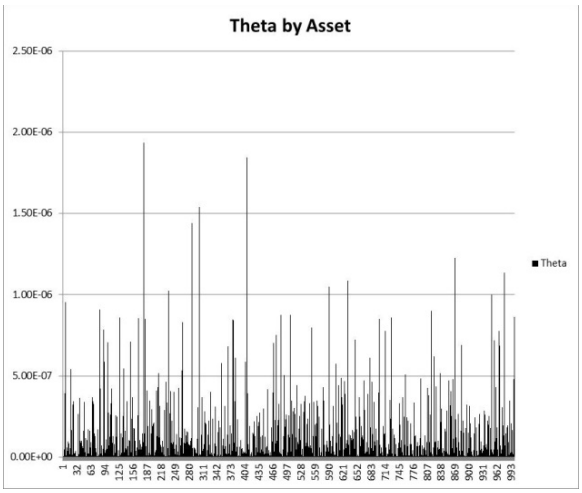


**Figure 1.1:** Unfiltered AVM Baseline Analysis Depicting Current Homeland Security Risk Profile

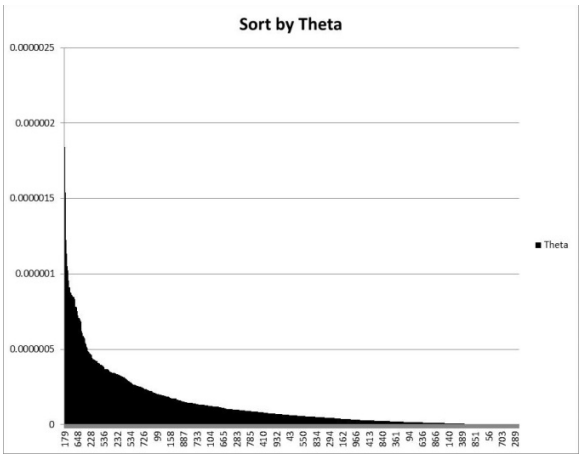


**Figure 1.2:** Baseline AVM Data Sorted by Theta Identifying Assets from Least to Most Vulnerable

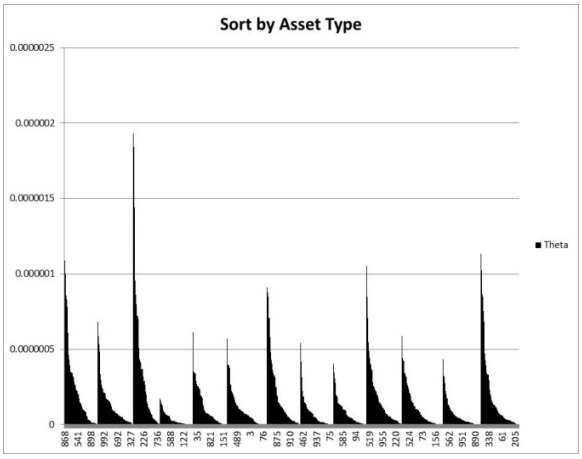


**Figure 1.3:** Baseline AVM Data Sorted by Asset Type Identifying Vulnerabilities by Infrastructure Sector

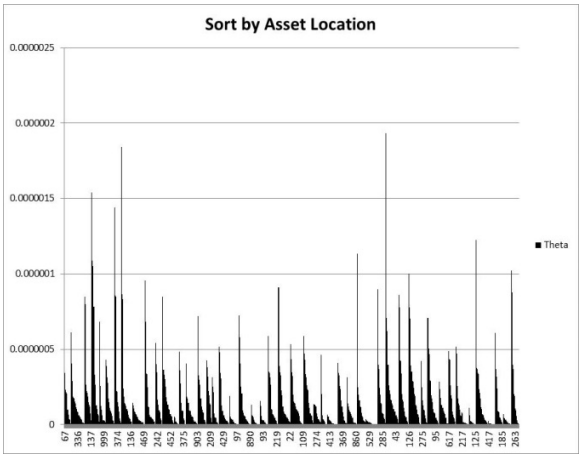


**Figure 1.4:** Baseline AVM Data Sorted by Asset Location Identifying Vulnerabilities by Region

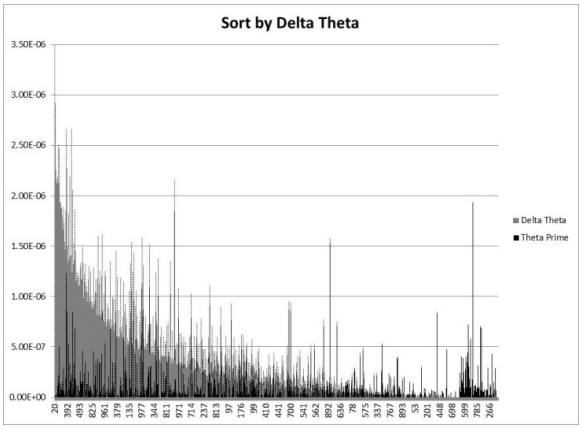


**Figure 2.1:** AVM Cost-Benefit Analysis Identifying Improvements in Order of Benefit (largest to smallest)

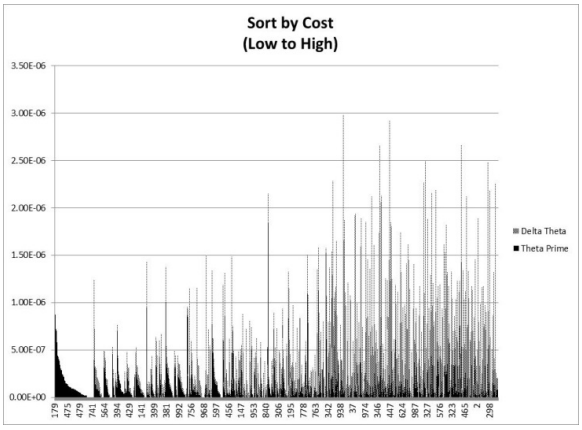


**Figure 2.2:** AVM Cost-Benefit Analysis Identifying Improvements by Cost (smallest to largest)

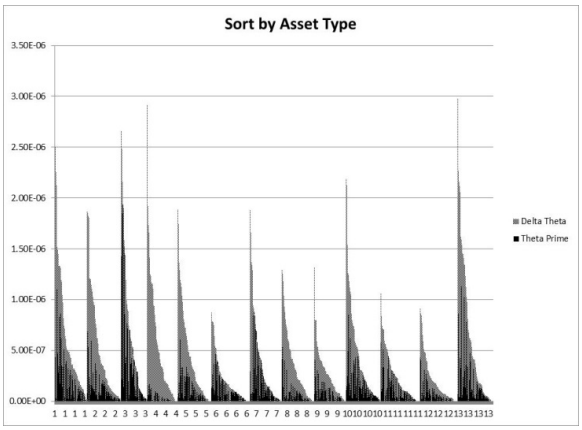


**Figure 2.3:** AVM Cost-Benefit Analysis Identifying Improvements by Asset Type

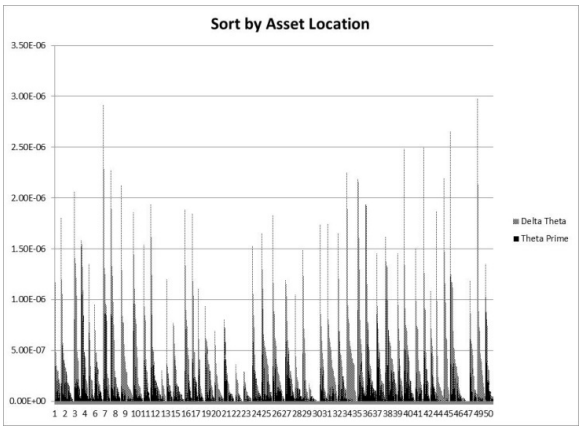


**Figure 2.4:** AVM Cost-Benefit Analysis Identifying Improvements by Region

AVM addresses many of the challenges to developing an adequate risk formulation for critical infrastructure. AVM avoids the problem of reliable threat estimation by adopting an asset-based vulnerability approach to risk management. Yet AVM is a comprehensive formulation addressing the five phases of emergency management: prevent, protect, mitigate, respond, and recover. All probability components in the AVM risk formulation, P(dis), P(def), P(den), and P(dim) make use of available empirical data facilitating documentation, transparency, and repeatability. The consequence component, %(dam), incorporates national economic and health data that capture the broader effects of both disruptive and destructive attacks. And AVM provides cost-benefit analysis and graphical presentation of the results in multiple formats supporting flexible decision strategies at all levels of management.

Working within the Risk Management Framework, AVM provides direction and coordination to help overcome current operational shortfalls. Beginning with Step Two of the framework, "Identify Infrastructure," AVM can help differentiate what infrastructure is critical from what is not. For example, shopping malls, race tracks, theme parks, and other questionable assets currently tracked by DHS would not be evaluated under AVM as they are inert, and by themselves could not be subverted or employed to create mass or debilitating effects. AVM baseline analysis conducted in Step Three, "Assess an Analyze Risks," provides a current risk profile of critical assets using the same capabilities and processes currently employed at DHS. By addressing risk components both "inside" and "outside" the perimeter of critical infrastructure, AVM provides a coordinating mechanism between the Risk Management Framework and National Preparedness System. Of course, there remains the question of voluntary versus mandatory data collection on the part of private industry. Most sectors identified in Table 2 are already federally regulated. It would not require much regulatory change to institute mandatory data collection from these sectors.[44] AVM cost-benefit analysis evaluates proposed improvement measures and identifies those providing the largest protective gain for the least cost. Thus AVM compares protective measures across all five phases of emergency management to determine the best investment option. AVM decision support tools present results in a flexible format that assists decision makers in recommending and justifying resource allocations in Step Four, "Implement Risk Management Activities." Through iterative application within the Risk Management Framework, AVM can measure and track investments and improvements over time.

## POLICY EXTENSION

As has been demonstrated, AVM can help unify and guide strategic investment decisions for protecting critical infrastructure. Critical infrastructure, though, is only half the problem. Weapons of mass destruction in the form of chemical, biological, radiological, and nuclear agents also present the opportunity for asymmetric attack. Referring back to Sandler and Lapan's findings in game theory (a coordinated defense is more efficient than an uncoordinated one) suggests that AVM should be extended to encompass both critical infrastructure and CBRN stockpiles. This will require interagency coordination between DHS, the Department of Defense, and the Department of Energy. Strategy coordination between executive departments is conducted at the highest level in the National Security Council.[45] Strategy formulation is shaped by National Security Strategy (NSS), which serves as a coordinating framework for federal agencies to prioritize resources and schedule activities to work towards common national goals.[46]

Current National Security Strategy reiterates the definition of homeland security promulgated in the 2010 *Quadrennial Homeland Security Review* as "a concerted national effort to ensure a homeland that is safe, secure, and resilient against terrorism and other and other hazards where American interests, aspirations, and way of life can thrive."[47] This definition places terrorism at the forefront of homeland security concerns. Such a suggestion belies the historical significance of 9/11. The United States had suffered terrorist attacks long before 9/11, but it wasn't until those attacks that homeland security became a national priority. What was unique about 9/11 that prompted the largest re-organization of US government since World War II and made homeland security part of the national lexicon? According to the 9/11 Commission, it was the "surpassing disproportion" of the attack. On September 11, 2001, nineteen men inflicted as much damage on the United States as the Imperial Japanese Navy on December 7, 1941.[48] 9/11 made manifest the unprecedented threat of domestic catastrophic attack accomplished through asymmetric means by small groups or individuals acting on their own behalf. The problem is not terrorism. Terrorism is defined as "any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments."[49] Terrorism is a motive. Certainly it played a role in the 9/11 attacks, but who is to say it is the only motive that could precipitate another such attack?

The current preoccupation with terrorism distracts attention from the real threat discerned by the 9/11 Commission: domestic catastrophic attack precipitated by subverting critical infrastructure or employing weapons of mass destruction. To effectively coordinate interagency efforts towards this problem, a new definition of homeland security should be considered. An alternative definition might be "to safeguard the United States from domestic catastrophic attack." This definition is more precise because it focuses on the specific problem of domestic catastrophic attack, directing attention to those means that make it possible. This definition is more comprehensive because it doesn't restrict the motives of the attackers. This definition is more discriminate because it distinguishes catastrophic attack from other forms of crime such as the mass killings at Newtown, Virginia Tech, and Columbine. Supported by AVM, the corresponding homeland security strategy becomes "maximize protective investments that minimize the probability of successful domestic catastrophic attack." This statement offers a concise strategy specifying "ends," "ways," and "means." Together with the new definition, they can help direct interagency efforts towards a unified homeland security strategy.

## FUTURE RESEARCH

While this paper has endeavored to present a comprehensive framework for defining and improving homeland security, some important implementation details remain for future research, and additional areas need to be explored.

First, a definitive taxonomy must be developed to help identify those things that can create a domestic catastrophic attack. DHS previously developed taxonomy for its National Asset Database.[50] Perhaps it can be adopted for this application. CARVER+Shock analysis has also been employed and may be sufficiently useful.[51] Related to this effort is defining "catastrophic attack." In 2002, the term "macroterrorism" was coined as "an act of terrorism causing at least 500 deaths, and/or property damage or economic loss exceeding $1 billion."[52] For reasons stated earlier, the word "terrorism" should be avoided as part of any definition of "catastrophic attack." As concern for homeland security began with 9/11, maybe it should become the benchmark: "Any deliberate act inflicting over 3,000 deaths or $40 billion in damages." This remains an area to be explored.

Understandably, the National Research Council places a premium on verifying and validating model results.[53] Again, the availability of historical data is problematic. In this regard, the NRC suggests one possible method recommended by the JASON scientific advisor group to "address smaller, well-defined, testable pieces of the larger problem."[54] How this might be accomplished is also an area for research.

A glaring omission from this proposal is how to treat natural disasters? Disaster response became a homeland security mission when FEMA was folded into DHS. The prevailing logic was that many of the same response and recovery capabilities for natural disasters were applicable to manmade catastrophes.[55] This rationale is supported by early work done at the Disaster Research Center (DRC) examining the demands a crisis imposes upon a social system and concluded that different agents may precipitate similar responses.[56] However, accounting for disasters in the same risk formulas for catastrophic attack presents a challenge in skewing the results because they have comparatively higher rates of probability and predictability. The problem is how to incorporate natural disasters into the analysis so they don't distract from the root problem of catastrophic attack. The National Research Council recommends keeping them separate.[57]

Finally, while AVM provides the means for developing coherent strategy, the next logical step is to explore among the alternatives. What investment strategy affords the greatest protection? Should DHS allocate funds towards (1) protective improvement measures based on least cost, (2) assets that are least protected, (3) regional improvements, (4) sector improvements, (5) improvements that provide the greatest protective gain, (6) assets with the highest consequences, or (7) some other strategy? Research has just begun to examine these strategies using AVM, and the preliminary results look interesting.

## CONCLUSION

This paper has examined current problems and underlying challenges to developing strategic direction for protecting critical infrastructure. It introduced an Asset Vulnerability Model to overcome these challenges and provide a coordinating framework facilitating strategic direction. Then, informed by insights from game theory, it proposed a policy framework that would extend AVM protection to encompass both critical infrastructure and domestic CBRN stockpiles. In this manner, AVM can account for investment of scarce national resources and lead the nation towards a unified homeland security strategy.

## ABOUT THE AUTHOR

**Richard White** *has a PhD in Security Engineering from the University of Colorado at Colorado Springs. He has taught various courses in homeland security since 2003, and directed homeland security exercises for United States Northern Command. He has a Bachelor's Degree in History and Master's Degree in Computer Science. He has published textbooks on military strategy, homeland security, and homeland defense. Richard may be contacted at rwhite2@uccs.edu.*

## NOTES

1. The White House, *Homeland Security Presidential Directive/HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection* (Washington, DC: Government Printing Office, 2003), 8.

2. Dick K. Nanto, *9/11 Terrorism: Global Economic Costs* (Washington, DC: Congressional Research Service, 2004), 2.

3. The White House, *HSPD-7,* 5.

4. Homeland Security Act of 2002, Pub. L. No. 107-296, 107th Cong. (2002).

5. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2013), 15-20.

6. National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, DC: The National Academies Press, 2010), 11.

7. John Moteff, *Critical Infrastructure: The National Asset Database* (Washington, DC: Congressional Research Service, 2007), 1-7.

8. Government Accountability Office, *Critical Infrastructure Protection: DHS could Better Manage Security Surveys and Vulnerability Assessments* (Washington, DC: United States Government Accountability Office, 2012), Summary.

9. Ibid., 14.

10. Todd Masse, Siobhan O'Neil, and John Rollins, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (Washington, DC: Congressional Research Service, 2007), 2-7.

11. John Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (Washington, DC: Congressional Research Service, 2011), 29.

12. Masse, O'Neil, and Rollins, *Assessment Methodology,* 14.

13. National Research Council of the National Academies, *Approach to Risk Analysis,* 2-3.

14. Department of Homeland Security, *Budget-in-Brief* (Washington, DC: Department of Homeland Security, 2014), 160-163.

15. The White House, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (PPD 21) (Washington, DC: Government Printing Office, 2013).

16. National Research Council of the National Academies, *Approach to Risk Analysis*, 11.

17. Masse, O'Neil, and Rollins, *Assessment Methodology,* 16.

18. National Research Council of the National Academies, *Approach to Risk Analysis*, 58-70.

19. Masse, O'Neil, and Rollins, *Assessment Methodology*, 16.

20. Ted G. Lewis, Rudolph P. Darken, Thomas Mackin, and Donald Dudenhoeffer, "Model-based Risk Analysis for Critical Infrastructures," in Francesco Flammini, *Critical Infrastructure Security: Assessment, Prevention, Detection, Response* (Ashurst, Southampton, UK: WIT Press, 2012), 4.

21. Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: John Wiley & Sons, Inc., 2006).

22. William L. McGill, "Critical Asset and Portfolio Risk Analysis for Homeland Security" (PhD diss., University of Maryland, 2008), 15.

23. Barry Charles Ezell, Stven P. Bennett, Detlof von Winterfeldt, John Sokolowski, and Andrew J. Collins, "Probabilistic Risk Analysis and Terrorism Risk," *Risk Analysis* 30, no. 4 (2010): 575-589.

24. McGill, "Critical Asset and Portfolio Risk Analysis," 16.

25. Masse, O'Neil, and Rollins, *Assessment Methodology*, 16.

26. National Research Council of the National Academies, *Approach to Risk Analysis*, 45, 47.

27. Ibid., 51.

28. Ibid., 64-65.

29. Ibid., 62.

30. Michael K. Lindell, Carla S. Prater, Ronald W. Perry, and William C. Nicholson, *Fundamentals of Emergency Management* (Washington, DC: FEMA, 2006), 23-26.

31. National Research Council of the National Academies, *Approach to Risk Analysis*, 51.

32. Ibid., 68-70.

33. P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* (Idaho National Laboratory, 2006).

34. Georgios Giannopoulos, Roberto Filippini, and Muriel Schimmer. *Risk Assessment Methodologies for Critical Infrastructure Protection Part I: A State of the Art* (European Commission Joint Research Centre, Institute for the Protection and Security of the Citizen, 2012).

35. McGill, "Critical Asset and Portfolio Risk Analysis," 15.

36. Giannopoulos, Filippini, and Schimmer, *Risk Assessment Methodologies,* 3.

37. The White House, *HSPD-7.*

38. Masse, O'Neil, and Rollins, *Assessment Methodology*, 17-18.

39. Ezell, et al., "Probabilistic Risk Analysis," 586.

40. Gordon Woo, "The Evolution of Terrorism Risk Modeling" *Journal of Reinsurance* (April 22, 2003), 7, https://support.rms.com/Publications/EvolutionTerRiskMod_Woo_JournalRe.pdf.

41. Todd Sandler and Harvey Lapan, "The Calculus of Dissent: An Analysis of Terrorists' Choice of Targets," *Syntese* no. 76 (Kluwer Academic Publishers, 1988), 249-254, http://link.springer.com/article/10.1007/BF00869591#page-1.

42. Government Accountability Office, *Critical Infrastructure Protection,* 9.

43. Giannopoulos, Filippini, and Schimmer, *Risk Assessment Methodologies,* 11.

44. Ted G. Lewis and Rudy Darken. "Potholes and Detours in the Road to Critical Infrastructure Protection Policy," *Homeland Security Affairs* 1, no. 2 (August 2005): 7, http://www.hsaj.org/?article=1.2.1.

45. Alan G. Whittaker, Shannon A. Brown, Frederick C. Smith, and Elizabeth McKune, *The National Security Policy Process: The National Security Council and Interagency System* (Washington, D.C.: Industrial College of the Armed Forces, National Defense University, 2011) 5.

46. Catherine Dale, *National Security Strategy: Legislative Mandates, Execution to Date, and Considerations for Congress* (Washington, DC: Congressional Research Service, 2008), 2.

47. The White House, *National Security Strategy* (Washington, DC: Government Printing Office, 2010), 15.

48. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: US Government Printing Office, 2004), 339-340.

49. Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Department of Homeland Security, 2002), 2.

50. Moteff, *The National Asset Database,* 9.

51. Food and Drug Administration, *Vulnerability Assessments of Food Systems: Final Summary Report* (Washington, DC: Food and Drug Administration, 2012).

52. Clive Williams, "Prospects for Macroterrorism," working paper presented at Pugwash Workshop on East Asian Security, Beijing, China, March 7-9, 2002, 9.

53. National Research Council of the National Academies, *Approach to Risk Analysis*, 12.

54. Ibid., 48.

55. Office of Homeland Security, *National Strategy,* 41.

56. Lindell, et al., *Fundamentals of Emergency Management,* 24-25.

57. National Research Council of the National Academies, *Approach to Risk Analysis*, 9.

# Preparedness Revisited: W(h)ither *PPD-8*?

Jerome H. Kahan

## ABSTRACT

*The most important purpose of Presidential Policy Directive (PPD-8) on national preparedness is to establish a foundation that can be adapted to and utilized by stakeholders of all kinds and at all public and private levels. PPD-8 appeared somewhat abruptly on the scene, essentially replacing Homeland Security Policy Directive (HSPD-8), which had accomplished much but suffered setbacks and stalled in its effectiveness. Perhaps the single most important step the Obama Administration can take at this point is to make as clear as possible to the nation not only about the need for, but also the challenges encountered in implementing a national preparedness plan. Efforts need to be redoubled if serious and sustained progress is to be made by the end of the President's second term. On balance, given that the fundamental elements of PPD-8 are similar to HSPD-8 but even more complex, the author's view is that the newer initiative faces the reality of ultimately being overwhelmed by powerful analytic difficulties and/or governance-related impediments – falling short of its goals, which may simply be too ambitious to realize.*

## DISCUSSION

On March 30, 2011, President Obama issued *Presidential Policy Directive (PPD-8),* a sweeping statement on national preparedness.[1] Its objective is "aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters."[2] One of the more important purposes of *PPD-8* is to establish a national-level foundation that can be adapted to and utilized by stakeholders at the state and local level.[3]

This punchy, six page *Directive* set in motion a complex set of supporting policies, programs, and procedures affecting the Department of Homeland Security (DHS) as well as all federal agencies with homeland security responsibilities. Critical components of this directive include developing a *National Preparedness Goal* (the *Goal*) that identifies core capabilities necessary for preparedness; employing a risk-informed capabilities planning method for prioritizing stakeholder capabilities; establishing a *National Preparedness System (NPS)* to guide planning and implementation activities needed to achieve the *Goal;* and producing a series of annual *National Preparedness Reports (NPR)* to assess progress.

As readers familiar with homeland security policies can attest, *PPD-8* appeared somewhat abruptly on the scene, replacing *Homeland Security Presidential Directive* (*HSPD-8)* signed by President George W. Bush in late 2003.[4] No reasons were given in the *Directive* or accompanying public statements for why it was decided to replace *HSPD-8*, nor were references made in *PPD-8* to the existence of such an earlier, similar directive.[5] It is difficult to avoid concluding that political forces as well as substantive needs were at work in driving *PPD-8*, designed to give President Obama full credit for moving forward on national preparedness, without explicit recognition of work done under the previous Administration.[6]

During the few years the new Directive has been in existence, the nation has experienced a series of devastating natural disasters and accidents, as well as the terrorist attack at the Boston Marathon.[7] National preparedness has once again become a prominent public policy issue.

The purpose of this article is to explore the question of how well *PPD-8* might meet its goals and objectives by the time the Obama Administration's second term is completed. It offers an understanding of the important

similarities and differences between *PPD-8* and the earlier *HSPD-8*.[8] Referring to the article's odd subtitle, our investigation can be framed as *whither PPD-8* (i.e., where is it bound?) or *wither PPD-8* (i.e., will it fade away?).

## CORE CAPABILITIES FOR PREPAREDNESS

Preparedness in the *PPD-8* context is taken to mean building the core capabilities "necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the Nation [… and a set of] prioritized objectives to mitigate that risk."[9] Using a capability-based planning process, *the Goal* identifies thirty-one different core capabilities aimed at turning each of five mission areas – prevent, protect mitigate, respond, recover – into practical policies and programs expressed as a set of prioritized objectives to reduce that risk.[10] *The Goal* also offers preliminary targets for each capability – so-called capability targets (TC) – that serve as a basis for assessing effective preparedness capabilities and identifying capability gaps.

Many questions have arisen about the way core capabilities are addressed under *PPD-8*.[11] National level core capabilities need to be based on credible evidence and/or systematic use of expert opinion, quantitatively or heuristically measurable, and tailorable to different users and situations**.** Without having been on the inside and in the absence of open sources that tell the full story, it is unclear how the *PPD-8* national core capabilities were constructed and how performance targets for each capability were developed.[12]

Speaking to a spectrum of stakeholders, *the Goal* stresses individual and community preparedness as fundamental to success, together with preparedness of governments at all levels and the private sector, including businesses and Non-Govermental Organizations (NGO).[13] Each member of the "whole community" is expected to achieve effective preparedness levels.[14]

A laudable goal of *PPD-8* is to establish measurable targets for core capabilities, scaled for diverse stakeholders. However, this is no easy task. As we will see, it is difficult enough to create a set of national preparedness core capabilities and with measurable targets, but far more challenging to adapt and apply these to the needs of all specific members of the whole community. Perhaps this helps explain why the *PPD*-8 implementation effort has faced difficulties in providing an analytically justified set of capabilities and targets that can support application across the diverse set of stakeholders and circumstances.[15]

## PREPAREDNESS RISK ASSESSMENTS

A strategic, national-level risk assessment (SNRA) was conducted as a necessary step soon after *PPD-8* was issued.[16] Results of the SNRA were used to formulate *PPD-8* national core capabilities and associated target priorities. The more important goal of the SNRA, however, was to provide the basis for developing a risk assessment method that could ultimately be used for the regions, communities, and multitude of local entities that comprise the nation, enabling them to prioritize their capability needs and gaps. Notwithstanding this expected follow-up role for the SNRA, a different path was followed to assist stakeholders below the national level in conducting risk assessments for preparedness.[17]

### *THIRA* Arrives

In April 2012, FEMA issued a *Threat and Hazard Identification and Risk Assessment (THIRA) Guide*.[18] Unlike the national-level thrust of the SNRA, the *THIRA Guide* is about community preparedness, a subject that has received great attention in recent years.[19] While the focus is on communities broadly defined, the *Guide* claims its approach can be adapted for use by all relevant entities below the federal level to support a diverse array of stakeholders – from all kinds of businesses, to owners and operators of large power faculties, to sprawling urban areas.[20]

The *THIRA Guide* itself notes the challenges in applying risk methodologies designed to deal with such a complex set of users as found in the range of communities across the nation,

each of which faces an array of relevant threats and hazards – sometimes in common but more often than not specific to its location, exposure, and other unique factors. Looked at from the opposite perspective, *PPD-8* calls for communities, as well as other entities, to each contribute to *the Goal* by preparing for risks that are most urgent and important from their perspective by employing core capabilities that can strengthen their resilience.

### Risk Assessment Process

A five-step process is presented in the *THIRA Guide* covering such issues as identifying likely threats and hazards, characterizing these challenges, conducting risk assessments, developing core capabilities and targets, and establishing preparedness measures to mitigate risk.[21] Execution of each of these steps is far from simple. Special expertise is needed to develop the needed methodological techniques for these risk assessments – estimating threats, developing scenarios, calculating consequences, producing capability needs, developing performance targets, and measuring mitigating effects. Not all required expertise might be available in each situation.[22]

With SNRA applied nationally and to federal agencies and *THIRA* available for all stakeholders below the federal level, *PPD-8* holds out great expectations for risk assessments as a tool to develop and prioritize core capabilities across the five mission areas. The idea is to use such tools for integrating contributions toward achieving *the Goal* from all stakeholders of different types and levels. This means not only combining risk results horizontally at the state level across the nation, but also aggregating these results vertically up the chain in order to characterize how well the system meets the broad national objectives presented in *the Goal*. As further explored below, this process faces such a high degree of significant challenges that it might prove to be impossible to execute in practice – a key issue the *Guide* does not address in a serious manner.[23]

In sum, the *THIRA Guide* is an informative document about risk in connection with preparedness planning for homeland security. However, it has an upbeat style that does not pay enough attention to how risk assessments in connection with *PPD-8* are extremely difficult to develop and execute with meaningful results integrated across the diverse range of stakeholders, missions, and scenarios. The conundrum is how to find an accurate way to conduct preparedness risk assessments that can be executed by key groups of stakeholders, notably typical communities.

## NATIONAL PREPAREDNESS SYSTEM

The *PPD-8 Implementation Plan* calls for the secretary of Homeland Security to develop a *National Preparedness System (NPS)* in coordination with other executive departments and agencies, and in consultation with state, local, tribal, and territorial governments, the private and nonprofit sectors, and the public. Published in late 2011 as an official FEMA document, the *NPS* is a means of outlining the process for how all stakeholders can move forward with their preparedness activities. This system is composed of six interlinked components: (1) identifying and assessing risk; (2) estimating the level of capabilities needed to address those risks; (3) building or sustaining the required levels of capability; (4) developing and implementing plans to deliver those capabilities; (5) validating and monitoring progress; and (6) reviewing and updating efforts to promote continuous improvement.[24]

### Nature of the *NPS*

Given such a broad scope and significant statement of purposes, the *NPS* is a surprisingly short, readable, somewhat informal publication, apparently aimed at interested citizens needing an overview of the process, rather than audiences of large institutions or homeland security professionals where a more thorough presentation would be suitable.[25] This might be due to an attempt to target the lowest common denominator of the diverse *NPS* audience..

In April 2013, FEMA published a new document focused on estimating capability

needs and gaps, known as the *Capability Estimation Comprehensive Planning Guide (CPG) 201*.[26] This document is said to support the second *NPS* component and replace *THIRA* in supporting the first component by enhancing but going beyond presenting a risk method *per se* and demonstrating the process by which communities could apply a risk assessment to determine resources needed to deliver core capabilities to the target levels.[27]

*CPG 201* describes in detail a method that leads to core capabilities for mitigating risk. The *THIRA Guide*, as noted earlier, needs more detail in explaining a risk assessment method if this is to be an operational rather than educational product. Unfortunately, the processes found in *CPG 201* suffer from the opposite problem of being too complex for real world application by communities, even with experts involved.[28] Balance is essential to ensure that stakeholders at all levels understand and apply risk assessments that result in countermeasures and mitigation strategies.

The third and fourth *NPS* components are fleshed out in a set of five National Planning Frameworks – one for each mission area – billed as instrumental to the success of *PPD-8* implementation in helping ensure the whole community can work together to achieve national preparedness.[29] Frameworks for almost all of the five *PPD-8* mission areas have been released.[30] Each Planning Framework is relatively comprehensive – defining relevant mission areas, summarizing the roles and responsibilities of members of the whole committee, and identifying relevant information to help with operational planning in delivering core capabilities to communities. The status of the two final components remains unclear.

### Status of the *NPS*

Much is riding on how the goals and objectives of *PPD-8* at the local level are turned into the reality of meaningful policies and cost-effective programs all based on serious planning efforts. The Government Accountability Office (GAO) concluded, "FEMA has made progress addressing that agency's earlier recommendation to develop a national preparedness assessment with clear, objective, and quantifiable capability requirements and performance measures, but continues to face challenges in developing a national preparedness system that could assist the agency in prioritizing preparedness grant funding."[31] In giving FEMA credit for making progress in managing *PPD-8* implementation, the GAO mentions publication of the *THIRA* Guide in 2012 and issuance of the first *National Preparedness Report (NPR)*, which will be discussed below.[32]

There remains work to be done, for example, in finalizing the full set of Frameworks to include validating and monitoring progress. Also needed are steps for reviewing all capabilities, resources, and plans based on updated risk assessments, and showing how the various components interact dynamically.[33] From an overall perspective, what needs to be secured and sustained is a strategy to build the proper capabilities for each group of stakeholders that are affordable and support the five preparedness missions. There is also a critical need, as will be further discussed, to develop a credible method for integrating and aggregating preparedness levels achieved by stakeholders that result in a national level preparedness assessment.

## NATIONAL PREPAREDNESS REPORT

*PPD-8* requires annual *National Preparedness Reports (NPR)* be submitted by the secretary of Homeland Security to the president. As officially expressed, "[L]ooking across all…core capabilities outlined in *the Goa*l, *NPRs* provide a national perspective on critical preparedness trends for whole community partners to use to inform program priorities, allocate resources, and communicate with stakeholders about issues of shared concern."[34] The first in this series of *NPR* was issued in March 2012 and the second a year later.[35]

### Understanding the *NPR*

The 2013 *NPR* focuses on homeland security programs and policies completed or underway as reported for 2012. It is an extremely

comprehensive document filled with detailed charts, graphs, and other forms of data presentation, as well as case studies, to support a series of eight overarching national trends and sixty-two key findings that align to the thirty-one core capabilities across the five *PPD-8* missions.[36]

The foundation for this analytic structure is the local assessments within each state and territory, which take the form of *State Preparedness Reports (SPR)*.[37] These contain state-level ratings of each core capability as high, medium, or low priority, based on results of *THIRA* risk assessments and capability estimates derived by aggregating results on risk-informed inputs from the *Sub-State Regions (SSR)* into which each of the fifty-six states and territories are supposed to be divided.[38] The *SSR* provide locally based assessments and data to the fifty-six states and territories that form draft *SPR* for FEMA to review. Once finalized, these are synthesized by FEMA to produce ten regional risk/capability assessments, which then lead to the national preparedness assessment captured in the *NPR*.[39]

The 2013 *NPR* findings incorporate preparedness information for each core capability from the 2012 *SPR* process, which serves as a baseline for assessing progress made in implementing preparedness efforts in support of *PPD-8* capability targets. There is no room in this article to cover the many details covered in the 2013 *NPR*. Worth highlighting, however, are the document's discussions of the following items.

- Progress made for core capabilities that support all five mission areas, notably Planning, Operational Coordination, Intelligence and Information Sharing, and Operational Communication.

- Accomplishments in other core capabilities with broadly relevant capabilities identified – notably, cybersecurity, recovery-focused core capabilities, and integration of individuals with disabilities and access and functional needs.

- Newly identified national areas for improvement under PPD-8, which have been part of preparedness initiatives for many years, including resilience of infrastructure systems and maturing the role of public-private partnerships.

With these sorts of outputs, the 2013 *NPR* represents a snapshot in time showing progress, current status, and issues to be tackled on the road to national preparedness.

## Value of the *NPR*

The first two *NPR* represent a pattern of slowly assembling the many pieces of national preparedness policies and programs at the stakeholder level as a means of providing a national perspective. The first *NPR* affirms the longer-term vision of this series of publications – notably, establishing "a routine, repeatable process that builds on other preparedness efforts, engages whole community partners, and provides meaningful, consistent input to show progress annually."[40] Constructing a truly representative, supported, and useful picture of something as complex as the national preparedness of the nation to meet a wide range of threats and hazards across the country at all levels of stakeholders will take time to demonstrate and develop for operational use in forming policies and priorities.[41]

The overall methodology employed to gather and assess data to generate what the *NPR* calls a national level assessment is complex and questionable. The first two *NPR* are filled with facts, figures, anecdotes, and observations, but do not represent credible, objective, supportable analysis. Using the *SSR* inputs, for example, both *NPR* rank order the percentage of states and territories rating themselves as high on a five-point assessment scale for planning, organization, equipment, training, and exercises. Here, as in other parts of the overall *PPD-8* process, we face the issue of false precision, where results might look good but be misleading by not accounting for the many uncertainties inherent in complex system behaviors. As preparedness efforts evolve and mature, there is recognition that '"future iterations of the *NPR* will increasingly reflect quantitative performance data and assessment results, as well as qualitative

program accomplishments that align with *the Goal."* [42]

However, at the end of the day, the path chosen by the *NPR* for fulfilling the need for a national preparedness assessment is likely to fail. Results based on non-validated data gathered at local levels within states will almost surely remain questionable, given the pilot program's results and more recent observations. Not to be forgotten is that *SPR* – instrumental inputs for the *NPR* – are built upon obtaining complete and credible assessments from the ground up for integration and aggregation. While lessons have been learned from earlier testing under a series of DHS-organized Pilot Capabilities Assessments (PCA), obtaining comprehensive and accurate sub-state and local preparedness inputs may not be feasible and, as self-assessments are used at this level, may not be credible.[43]

One final methodological concern is that the *NPR* are based upon self-assessments by the states. Even if relying upon what seems to be comprehensive and consistent data – an assumption that cannot be taken for granted – such self-assessments raise serious concerns over objectivity and credibility in Congress and with the stakeholder community and the public at large. Shifting to an independent assessment might be a wise step to take.

## TWO BIG ISSUES

The GAO's conclusion that progress has been made towards reaching *PPD-8*'s goals and objectives are correct as far as they go.[44] However, with its public face and in open testimonies as well as published documents, the Administration has yet to directly confront and discuss in some detail the inescapable fact that this program continues to face enormous challenges. Quite the opposite, *PPD-8* and its key implementing documents tend to present preparedness plans and actions as relatively easy to execute by any member of the whole community — from individuals to large organizations.

This approach is misleading. The public should be made aware at least of the two largest hurdles to overcome before national preparedness can in fact be achieved: the difficulties in understanding the level of preparedness and the dilemmas faced in dealing with governance issues.

### Wicked Problem

When turning from words to implementation, the *PPD-8* approach to national preparedness reflects the characteristics of what is called a "wicked problem" – hard to define, delimit, and understand, reflecting uncertainties, and having many moving parts that interact often in unknown ways.[45] The sheer complexity of the multifaceted *PPD-8* implementation strategy has already been demonstrated in our discussions of such elements of the *Directive* as capabilities-based planning, risk assessments, and the National Planning Frameworks. For this reason, practical assessment of national preparedness will involve a multivariable, multi-dimensional process of measuring, assessing, and aggregating the performance of many different capabilities deployed by many different entities at many different stakeholder levels to address five different mission areas. Such wicked problems are typically not prone to analytic solutions leading to useable outcomes.

One aspect of wickedness in *PPD-8* has to do with the extremely difficult analytic task of developing a set of measurable preparedness national capabilities that can be adapted to the needs of state and local stakeholders across the whole community with different threats and hazards and capabilities. Is it really expected that each of the ten FEMA national regions as well as the fifty-six states and territories, hundreds of metropolitan areas, thousands of cities, and tens of thousands of communities will have the interest, capabilities, and resources to produce such a plan? How can these pieces be integrated into a coherent nationwide puzzle that portrays a credible picture of preparedness? What about incorporating cooperation with international partners, especially Canada and Mexico? As put by the GAO, "until FEMA develops clear, objective, and quantifiable capability requirements and performance measures, it is unclear what capability gaps currently exist and

what level of federal resources will be needed to close such gaps."[46]

More fundamentally, multi-level nationwide preparedness capability assessments, such as represented by the *PPD-8* initiative, pose complex analytic and organizational challenges. While there are existing methods for hierarchical data assessments – including the concept of multi-stage sampling and selective indicators – these approaches have their own limitations, do not deal directly with homeland security preparedness, and cannot easily be adapted to the problem *PPD-8* seeks to address. A 2007 report by the *Homeland Security and Analysis Institute* provides a useful initial "proof of concept" examination of a layered homeland security preparedness approach. It "presents a method for developing preparedness capability assessments that integrate and aggregate assessments across all levels of responsibility, ultimately resulting in a nationwide assessment."[47] It demonstrates just how complex and virtually undoable such problems become when examined closely.

Preparedness can be said to have one reality at the federal level, another at the regional, another at the state, and still another at the local level. For example, the risks seen by a medium-sized Midwestern community would be very different from those seen by coastal urban areas that are different still in regions such as the Pacific Northwest. The challenge faced is how to form a top-level aggregated assessment across all levels of government and non-governmental entities, aimed at providing the president and Congress with an overall rating of how well the nation as a whole is prepared to meet major terrorist and natural disaster challenges. This is what the *NPR* ultimately aims to develop. It is not clear that there are other fundamentally different ways of trying to gauge national preparedness.[48]

Regrettably, as noted above, the *PPD-8* implementing documents do not clearly address the wickedness of the challenges faced. We find some instances where this issue is noted; for example, *THIRA's* acknowledgement that risk assessments can be complicated. We also find a few broad statements made in passing within which lurk extremely complex analytic challenges that are not mentioned, such as, "[t]he five mission areas exist along a continuum, and t*here is a dynamic interplay between and among them* and even some commonality" [emphasis added].[49] However, the set of *PPD-8* documents as a whole do not do justice to the many analytic obstacles that need to be overcome in key assessment steps that need to be taken.

As a final point, *HSPD-8* has also been characterized also as a wicked problem – though with more moving parts, *PPD-8* may well be a more wicked problem to solve than *HSPD-8*.[50]

## The Governance Dilemma

*PPD-8* implementation has been trying to engage all members of the whole community in a sustained manner, as preparedness requires constant attention as threats, circumstances, and requirements change. Without question, jurisdictions, agencies, and organizations at all levels would benefit from a standardized but flexible method to plan for, assess, and track preparedness within a common analytic framework.

Given our federalist system, however, governance issues tend to arise when interactions take place among responsible authorities at all levels in developing capability assessments. States and local jurisdictions often resist what they perceive as federal imposition of a one-size-fits-all set of homeland security objectives, standards, and procedures. Early in the process of *HSPD-8* implementation, for example, a senior DHS official observed that it would require a "'consensual community' to accept and apply this approach, recognizing that endorsement of this process across all jurisdictions would be complicated and entail, *inter alia,* concerns over loss of sovereignty in some states."[51]

Difficult as it may be, *PPD-8* implementation, as *HSPD-8* before it, must somehow seek to balance the federal government's responsibility for the nation's safety against the freedom for state and local jurisdictions to govern at their respective levels. There is no simple solution. Some argue that a top-down approach

intended to assist, but not direct, planning and measurement is, by definition, antithetical to a federalist form of government. Others argue that bottom-up approaches have no coherence and may not have significant impact at higher levels.

The answer lies in between and is a function of the particular issue. In connection with *PPD-8*, perhaps Christopher Bellavita is right in observing that putting up with all the "messiness, inefficiency and other faults" as the price to be paid for living within a federalist system of governance formed the main hurdle to be faced in the attempt to implement [...the] earlier [...*HSPD-8*] preparedness strategy.[52]

## CONCLUSIONS

The preparedness program called for by *PPD-8* is extremely ambitious, with implications for how to proceed in future years. Expanded efforts can be made by the Obama Administration to place higher policy priority on and provide greater resources for getting the nation in a better preparedness position by the end of the president's second term. On the other hand, even with such efforts, national preparedness may not move demonstrably ahead over the next few years.

### Keep Trying

The game is not over. Further initiatives can and should continue to be taken to increase the chances of *PPD-8* making a sustained imprint on national preparedness policies, programs, perceptions, and priorities. At the moment, however, the single most important step the Obama Administration can take is not only to make clear to the nation the need for enhancing our preparedness in the face of terrorist threats and natural disasters, but also to acknowledge the major challenges that must be overcome in implementing a national preparedness plan.[53] The aim would be to reinforce the need for the whole community to work on this problem, adapting solutions to local and regional conditions within broad federal guidelines, while at the same time seeking to lower expectations regarding the outcome being sought by the time this Administration leaves office. Care should be taken to acknowledge the existence of large uncertainties and complexities in understanding the dangers facing the nation from major natural disasters and terrorist attacks as well as the best ways to mitigate these challenges to reduce risk while adhering to our federalist system of governance.

Examples of specific steps to be considered in improving preparedness include:

1. **Improving Stakeholder Engagement.** The Administration has been working with federal, state, and local governments as well as NGO and the private sector to realize the objectives of *PPD-8*.[54] However, it is not too late for DHS to take even more vigorous steps to engage all key stakeholders in the *PPD-8* process. In doing so, policies and programs need to remain sensitive to the need for states and local communities to act in their own interests as long as this is not inconsistent with the thrust of the new preparedness strategy. More effort ought to be put into creating greater incentives for the private sector to enhance their preparedness, building on programs currently in place, which would offer financial assistance, tax write-offs, and the equivalent of a "good preparedness seal of approval" known as *Resilience STAR*TM.[55] Practically speaking, resource limits will likely constrain how much effort can be put into more vigorous stakeholder engagement efforts.[56]

2. **Fixing the *NPR*.** The second report, issued two years after *PPD-8*, is much improved over the first edition, which sought to assess preparedness progress while *PPD-8* was replacing key elements of *HSPD-8*. Future *NPR* should be more heuristic than the first or second, with less false precision using low confidence numbers and typically unreliable percentages. They should manage expectations by acknowledging the difficulties of implementing and measuring preparedness progress at all levels, especially at the national level. Moreover, rather than a fruitless pursuit of practically unattainable performance

goals that presumably would *eliminate* risk, subsequent *NPR* ought to focus on the *relative* progress of *PPD-8* toward the desired end state of *managing* risk. No matter how well put together, however, if subsequent *NPR* remain self-assessments, they will continue to suffer from credibility problems. Finally, some mechanism needs to be found for developing an independent assessment of the first draft of each *NPR* as produced by FEMA.[57]

3. **Developing an *NPS* "Do it yourself" Kit.** The challenge here is how to find a balance between the somewhat simple 2011 version of the *NPS* and what appears to be the production of each of the six *NPS* component parts in great detail.[58] One idea would be an updated *NPS* that again pulls together all parts of this system in the form but this time in the form of a "do it yourself kit" for non-federal public and private users. This document would offer easy-to-follow steps for each of the six components that reflect decent accuracy and note unavoidable uncertainties. Sections of the kit would include examples for different types of users of appropriate adaptation and prioritization of the *PPD-8* national-level core capabilities and targets for use in different categories of stakeholders, ranging from communities, to large urban areas, states, and regions comprised of many states. It would then go further to at least illustrate how risks, capability gaps, and solutions to enhance preparedness can be aggregated from local, to sub-state, to state levels across the nation. This can then lead to risk assessments for the ten FEMA Regions and ultimately provide national assessment input to the president via a series of *NPR*.[59]

## Success May Not Be Around the Corner

Steps such as those summarized above can be useful. However, the experience thus far with *PPD-8* implementation suggest that, as a practical matter, this initiative does not have a high chance of succeeding in reaching its stated goal. Many experts believe that *HSPD-8* failed to make significant and sustained progress in meeting its preparedness objectives for the nation. By the time *PPD-8* was published, there were examples galore of issues that led to *HSPD-8* showing serious signs of failure.[60] If this were true for the less complex *HSPD-8*, it would seem to be a serious warning flag for the success of *PPD-8*.[61] Indeed, as noted in our discussion, *PPD-8* may prove to be more difficult to implement than *HSPD-8* because of its greater number of inherent complexities and the early confusion caused by an abrupt switch from one preparedness strategy to another.

*The Goal* defines success in the *PPD-8* context as "a secure …and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[62] Looked at another way, success is not only aimed at ensuring preparedness for all stakeholders across the country at all levels, but also designed to help reach the more expansive goal of ensuring that the whole community is prepared to cope with successful terrorist attacks and major national-level disasters.

While well expressed, a key question associated with *PPD-8* is how will success be measured? It is doubtful that there will be a magic measuring stick invented that could tell the president, the Congress, and the nation as a whole, how well *PPD-8* implementation is going and how close the total efforts made under this *Directive* might come to reaching the rather broad end-state quoted above by the time the president leaves office. It would be misleading at best and dangerous at worst if the attempts to rate progress via the methods employed by the *NPR* are relied upon, even if best efforts are made to find better tools. It is the nature of wicked problems that issues such as success and failure are difficult if not impossible to assess in credible and objective ways.

We are clearly faced with a very wicked, wicked problem in seeking to develop a truly strategic view of the nation's preparedness. As discussed, this would entail a horizontal and vertical hierarchical, analytically based

assessment method that poses significant analytic and governance challenges and may not be doable as a practical matter.

Realistically, all that can and should be done is to chip away at the problem at all levels, employ only well-tested and cost effective measures, and temper expectations. At the national level, this is the time to objectively debate the effectiveness and efficiency of our national preparedness strategy and capabilities. What is needed is not be some sort of pseudo-analytic formula for measurement, but an informed national perception of how well *PPD-8* and other preparedness policies and programs have improved the country's preparedness against a range of likely threats and hazards with nationwide implications and a set of low likelihood incidents that can cause high consequences.

### The Road Ahead

If *PPD*-8 shows significant progress by the time President Obama leaves office, an incoming administration might decide to adopt a low-key effort that keeps slugging away at improving national preparedness. Less probable, but possible, would be a decision to undertake yet a third effort with the same thrust but a brand new name and number in the tradition of *PPD-8* and *HSPD-8* before it.

If it appears that substantial progress in developing a feasible and meaningful national preparedness program has *not* been made by the time Obama leaves office, however, a new administration might simply decide that no credible nationwide approach to preparedness is workable in this large, diverse country with its special governance structure. This would of course allow for communities and all stakeholders to continue to prepare themselves as best they can with help from the federal government, but with no attempt to forge a common strategy and measure overall national preparedness.

After diving into and digging out of this issue, this article argues that *PPD-8* faces the reality of ultimately being overwhelmed by similar and equally powerful analytic difficulties and/or governance impediments as the *HSPD-8* initiative before it. In sum, regarding overall national preparedness strategies, to the extent that proverbs can proscribe policy, it can be said that if a second attempt to attain sufficient and sustained national preparedness through *PPD-8* is seen as not succeeding, it might *not* make sense to "try, try,[...and] try again."[63]

## ABOUT THE AUTHOR

***Jerome Kahan*** *is currently an independent writer and analyst. He was formerly a distinguished analyst at the Homeland Security Studies and Analysis Institute in Arlington, VA. Mr. Kahan has been in the national security, arms control, and homeland security fields for over forty years —including twenty years with the Department of State, where he held positions on the policy planning staff and as deputy assistant secretary with the Political-Military and Intelligence Bureaus and served as counselor at the American Embassy in Turkey. He worked for many years with non-governmental research organizations, including the Brookings Institution, the Center for Naval Analyses, and Systems Planning and Analysis. He has written and/or contributed to a number of books, published articles in a variety of journals, taught at the Air Force Academy, and served as an adjunct professor in the School of Foreign Service at Georgetown University. Mr. Kahan holds a Master's Degree in Electrical Engineering from Columbia University, with bachelor's degrees from Queens as well as Columbia College. He has also been a member of the Council on Foreign Relations and the International Institute of Strategic Studies.*

## NOTES

1. The White House, *Presidential Policy Directive (PPD-8)* (Washington, DC: Government Printing Office, March 30, 2011).

2. Ibid., 1. Although resilience is included in this definition, PPD-8 and its implementing documents do not apply this concept as a major strategic driver or practical planning factor. The focus is on preparedness, which produces resilience as one of its outcomes.

3. As put by the *Directive*, while *PPD-8* is "intended to galvanize action by the Federal Government, it is also aimed at facilitating an integrated, all-of-Nation, capabilities-based approach to preparedness [...as] national preparedness is the shared responsibility of all levels of government, the private and nonprofit sectors, and individual citizens." Ibid., 1.

4. The White House, *Homeland Security Presidential Directive (HSPD)–8, National Preparedness* (Washington DC: Government Printing Office, December 17, 2003).

5. Those in the preparedness business when *PPD-8* was issued were surprised. As an example, an apparently disgruntled FEMA employee offered the following observations via a *PPD-8* website created by this agency: "Since HSPD 8 is now replaced by PPD8, what has this done in regards to the training and direction that many of us have spent years teaching? ...How much time and money will it draw away from other areas while 80% to 90% of the current training and documentation is changed to reflect these small changes? My question is, is it really worth the time and effort to go through all of this? ...What were the driving factors to make this change? Were they driven by reality? Or was this just an expensive and time-consuming political stunt?" Promoting Preparedness - (FEMA) - by IdeaScale fema. ideascale.com/a/ideafactory.do?id=14692&mod.

6. As pointed out by a homeland security expert, the *PPD-8* initiative does not refer to or recognize "what has and has not been accomplished since the last major preparedness directive was issued... [and] reads as though the past seven years never happened." See "Homeland Security's Presidential Policy Directive: Two Steps Backwards," Jena Baker McNeill and Matt A. Mayer, Heritage Foundation*, April 14, 2011,* www.heritage.org/.../two-steps-backward-homeland-security-presidential

7. Recent natural and accidental disasters across the nation include massive wildfires, floods, and hurricanes, as well as the fertilizer plant explosion in Texas.

8. A full side-by-side comparative analysis of these two directives is beyond the scope of this article, but important insights can be gained by looking back at *HSPD-8* in considering the future of *PPD-8*.

9. *PPD-8,* 1. A capability is "the ability to provide the means to accomplish one or more tasks under specific conditions and to specific performance standards. A capability may be achieved with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the intended outcome." Jared T. Brown, *Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress* (Washington DC: Congressional Research Service, October 21, 2011), 15.

10. Capabilities-based planning, used by the Department of Defense and in the private sector, entails planning under uncertainty to provide capabilities suitable for a wide range of future challenges and circumstances. It involves working within a framework that considers costs and sustainability and necessitates prioritization and choice to enable officials at all levels to make informed choices that best strengthen homeland security capabilities. As applied to homeland security, capabilities-based planning serves as an analytic method for conducting risk assessments under uncertainty against all-hazard threats to develop the means to respond to a wide range of potential challenges and circumstances. For groundbreaking work on the challenges faced in applying capabilities based planning to homeland security see Sharon Caudle, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community," *Homeland Security Affairs* I, no. 2 (Fall 2005), http://www.hsaj.org/?article=1.2.2, and also her *Homeland Security and Capability Based Planning: Improving National Capabilities* , Thesis, Naval Postgraduate School, Monterey, CA, September 2005, 49-50, http://www.dtic.mil/dtic/tr/fulltext/u2/a439372.pdf.

11. Developing core capabilities with associated targets, and seeking to adapt these to the diverse needs of all relevant stakeholders, posed major analytic and governance related difficulties during the *HSPD-8* era. The Target Capability List (TCL) was surrounded in controversy from the start. The *TCL* established national targets for performance and resource capabilities across the prevent, protect, respond, and recover mission areas. Seventy-one critical capabilities were initially identified, which differ in substantive detail as well as numbers from the thirty-one TCs developed for PDD-8. Moreover, the *TCL* issued under *HSPD-8* contained only thirty-seven of the seventy-one initial capabilities.

Developing, implementing, and evaluating the core capabilities associated with *PPD-8* are likely to experience many of the same inherent challenges that were experienced in the earlier *HSPD-8* attempt to realize preparedness core capabilities. For groundbreaking work on the challenges faced in applying capabilities based planning to homeland security see Sharon Caudle, as referenced above.

12. Relying on unclassified and unrestricted information, a good faith effort was made by the author to discover the process by which the core capabilities were constructed and performance targets developed under *PPD-8*. Non-governmental analyses are few and official sources are overly general, for example, *Learn About Presidential Policy Directive-8,* FEMA.govwww.fema.gov/learn-about-presidential-policy-directive-8. One useful source is the statement by Sharon L. Caudle, Ph.D., Younger-Carter Distinguished Policymaker in Residence and Visiting Lecturer, The Bush School of Government and Public Service Texas A&M University, House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management: *Is DHS Effectively Implementing a Strategy to Counter Emerging Threats?* February 3, 2012. As to setting numerical target levels for certain TCs, such attempts convey a sense of credibility and precision, are often not well supported, and can be highly misleading. For example, for the capability designated " Screening, Search, and Detection," the Target Capability found in *the Goal* is conveyed as "screen *67,500 people* associated with an imminent terrorist threat or act using technical, non-technical, intrusive, or non-intrusive means.", *National Preparedness Goal* 1st Edition, Table 2 (Washington DC: September 2011), 3. In such situations, the author likes to cite the saying attributed to John Maynard Keynes, "it is better to be roughly right than precisely wrong." http://www.goodreads.com/quotes/265041-it-is-better-to-be-roughly-right-than-precisely-wrong.

13. "Every member of the entire nation takes actions to strengthen their preparedness by adapting and applying [… the national ] core capabilities for each mission area as relevant to the threats and hazards they expect to experience—including individuals, communities, the private and nonprofit sectors, faith based organizations, and Federal, state, and local governments. By so doing, they not only improve their preparedness, but also make overall national preparedness stronger." *The Goal*, 1.

14. The "whole community" is the current term for characterizing the different types and sizes of stakeholders not only at federal level, but across the country to include private as well as public stakeholders at state and local government levels, a wide range of cities/urban areas and communities, large and small private businesses, non-governmental organizations (NGO), and concerned citizens and families. It has largely replaced the term "Homeland Security Enterprise."

15. One major impediment to success, as put by GAO two years ago is the lack of "national preparedness capability requirements based on established metrics to provide a framework for… assessing federal, state, and local preparedness capabilities against capability requirements to identify capability gaps for prioritizing investments in national preparedness." See *Measuring Disaster Preparedness: FEMA Has Made Limited Progress in Assessing National Capabilities,* Testimony by William O. Jenkins, Jr., GAO Director Homeland Security and Justice Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, Statement United States Government Accountability Office (Washington DC. March 17, 2011), 9-10. This continues to be an issue needing to be resolved.

16. The *PPD-8 Implementation Plan* specifically calls for the secretary of Homeland Security "to conduct a strategic, national-level risk assessment to identify the relevant risk factors that guide where core capabilities are needed and develop a list of the capabilities, […capability targets], and associated performance objectives for all hazards that will measure progress toward their achievement." *Implementation Plan for Presidential Policy Directive 8: National Preparedness* (Washington, DC: May 2011), 2. Against a five-year planning period, the *SNRA* assessed risk as a function of frequency and consequences for a set of 24 national-level events. The methodology incorporated data from a variety of inputs, including leveraging existing models and assessments, the historical record, and expert judgment. *SNRA* produced risk-informed results were used to develop and prioritize the national core capabilities. What we know is based on an unclassified summary issued by FEMA, *the Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation* (Washington DC: FEMA, December 2011), http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf. Without access to classified materials, it is not possible to check how these risk outcomes shaped national capabilities and targets and whether any capabilities were solidified without flowing from a credible risk assessment.

17. Perhaps it was recognized, upon a closer look, that adapting the *SNRA* to regional and local levels is not easily accomplished. A single methodology might not be applicable. Even with a credible national level risk assessment using the national core capabilities and a set of generic scenarios, there are special challenges in determining the methodology, level of detail, and data requirements to support risk assessments by communities and other public and private entities in various locations exposed to different threats and hazards.

18. *Threat and Hazard Identification and Risk Assessment (THIRA) Guide,* First Edition, CPG 202 (Washington, DC: Department of Homeland Security, April 2012). *PPD-8* is based on the premise that all communities need to conduct risk assessments of the threats and hazards they face in order to make informed decisions about the capabilities they must deploy in order to manage risk.

19. For example, see the work done by the Community and Regional Resilience Institute (CARRI), www.resilientus.org/ See also, Jerome Kahan , et al, *Community Resilience Profiles: Assessment and Evaluation, Final Report,* Homeland Security Studies and Analysis Institute, December 19, 2011, www.dhs.gov/homeland-security-studies-and-analysis-institute-hssai

20. There are many public and private entities below the national level besides communities, such as the interstate regions, individual states and territories, major metropolitan areas, all kinds of smaller jurisdictions and localities as well as different slices of critical infrastructure, hosts of NGO, and multitudes of large and small businesses.

21. *THIRA,* 3.

22. Even experts find it challenging to develop threat assessments requiring estimates of likelihoods and consequences set within credible scenarios for each stakeholder facing particular dangers. See National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis* (National Academies Press, 2011). On-the-ground assistance can be of great value in adapting and applying normative risk principles to local capability needs, but DHS cannot afford to send experts to all the cities, communities, and localities across the nation, let alone meet the needs of concerned citizens.

23. More specifically, *the Guide* fails to properly articulate address whether the proposed risk method is feasible when applied by a wide spectrum of users facing different threats and circumstances; the degree to which the varied technical abilities of users are sufficient to execute the method and apply results; and the implications of differing levels of stakeholder interest in high priority risk assessments for preparedness planning. Another impediment integrating risk assessments from top to bottom is the fact that risks aggregated upwards to the national level would be based on *THIRA*, which turns out not to be directly related to the earlier top-down *SNRA* effort!

24. FEMA, *National Preparedness System*, (Washington DC: Department of Homeland Security, November 2011) wwwfema.gov/pdf/prepared/nps_description.pdf . In the interest of keeping the public informed as the NPS moves forward, FEMA has a website that explains the components of the *NPS* and provides specific tools and resources to help communities and individuals through the *NPS* cycle. At http://www.fema.gov/national-preparedness-system

25. The *NPS* uses the word "you" quite often, as in "you coordinate your plans with other organizations," and uses informal expressions such as "Now it's time to see if your activities are working as intended." This tone has the ambience as if someone from FEMA is having a nice chat about preparedness in someone's living room.

26. *Capability Estimation Comprehensive Preparedness Guide (CPG) 201,* second edition, FEMA, April 2013.

27. C*ommunity* refers broadly to all types of communities, including communities of practice, communities defined by geography (regions and jurisdictions), and communities with other shared interests. *Resources* typically refers to personnel, teams, facilities, equipment, and supplies, but is here expanded to include plans, procedures, strategies, training, exercises, programs, systems, technologies, services, funding, authorities, laws, ordinances, and policies." *CPG*, 2.

28. The following passages, drawn somewhat arbitrarily from different pages of *CPG 201* give a flavor of some of the issues involved. "This analysis compares current resource levels to the desired capability targets… or each capability target, communities should examine current resource levels using information from real-world incidents, assessments, planning processes, and exercises. This examination may involve additional information gathering and research in partnership with whole community partners, including those from the private and nonprofit sectors, faith-based organizations, and community-based organizations… This strategy should take into account existing community resources, resources from non-traditional partners, mutual aid agreements and partnerships, partners at other levels of government, and, lastly, grant investments. Communities should pull from and consult with strategic, operational, and tactical plans, including emergency operations, hazard mitigation, comprehensive/land use, economic development, housing, resource protection, transportation, and recovery plans; after action reports, improvement plans, and other capability assessments; local and regional planning groups…; groups representing those with disabilities and others with access and functional needs; trusted public-private relationships and working groups such as local business and industry groups…, and laws, authorities, policies, and procedures…When communities successfully implement this strategy, the *THIR*A capability targets may need to be reduced. …This would then require revision of this capability

estimation process." As a former (Adjunct) Professor, the author can only remind the reader that there will be a short Q&A test on this material!

29. The Frameworks follow the whole community approach to preparedness, which recognizes that everyone can contribute to and benefit from national preparedness efforts. Each Framework explains the guiding principles and scope of mission area; summarizes the roles and responsibilities of each part of the whole community; defines the mission area's core capabilities, along with key examples of critical tasks; defines coordinating structures—either new or existing—that enable the whole community to work together to deliver the core capabilities; describes the relationships to the other mission areas; identifies relevant information to help with operational planning; and provides information that state, local, tribal and territorial governments can use to revise their operational plans. See *National Planning Frameworks* at FEMA.gov www.fema.gov/national-planning-frameworks

30. The National Disaster Recovery, National Prevention, National Mitigation Framework, and second edition of the National Response Framework have been released, with the National Protection Framework to be released later to conform with the evolution of national protection policy. Ibid.

31. *FEMA Has Made Progress, but Additional Steps Are Needed to Improve Grant Management and Assess Capabilities,* Government Accountability Office, GAO-13-637 (June 25, 2013), 1, at http://www.gao.gov/products/GAO-13-637T

32. In 2011, the Congressional Research Service (CRS) highlighted a number of issues that Congress may wish to oversee as the Administration "creates and implements" its many elements. These include "evaluating how *PPD-8* policies conform with statute; how federal roles and responsibilities have been assigned to implement and execute *PPD-8* policies; how non-federal resources and stakeholders will be impacted by national preparedness guidance; and how the overall federal budget may be reprioritized by a new national preparedness goal." Jared T. Brown, *Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress* (Washington, DC: CRS, October 21, 2011), Summary.

33. On this point, in what is surely an understatement, *CPG 201* notes that *NPS* components continuously affect each other, but does not demonstrate these dynamics. What is presumably meant are such interactions as TSA, CBP, and ICE work together at airports to detect and deal with the risk of terrorists entering the country using illegal immigration documents when arriving in country.

34. NPR 2013, Fact sheet

35. *National Preparedness Report* (Washington, DC: Department of Homeland Security, March 30, 2012, and *National Preparedness Report,* March 30, 2013.

36. The 2013 *NPR* relies upon approximately 1,400 sources and 3,200 measures and metrics that contribute to analysis of the core capabilities and related targets identified in *the Goal.* Inputs were elicited from all types and levels of public and private partner, which are then systematically synthesized by FEMA into observations on capability progress achieved.

37. *State Preparedness Reports (SPR*) have been produced annually starting in 2007 under the HSPD-8 framework. The results of the *THIRA* risk and capability estimation processes for states and territories receiving Federal preparedness assistance are reported annually through the State Preparedness Report (SPR). They initially reflected self-assessments of how the *TCL* was meeting its thirty-seven target capabilities under *HSPD*-8 initiative, changing as the initial *TCL* changed, and refocusing themselves as *PPD-8* replaced *HSPD-8* with its thirty-one core capabilities and targets. FEMA published an online, interactive tool that guides states and territories through the *SPR* assessment process to ensure consistency of data and continued implementation of the capability assessment aspect of the National Preparedness System. See *State Preparedness Report Guidance,* Fiscal Year 2008, Department of Homeland Security.

38. The *SSR* concept arose in December 2004, when the Office of Domestic Preparedness (ODP) requested that states designate *Sub-State Regions* for homeland security. Reflecting their own histories and preferences, different states have chosen to build SSRs using a variety of structures and organizing principles. Many *SSR* are organized according to emergency preparedness needs keyed to natural disasters as opposed to terrorist threats. Some states designate *SSR* only for periodic preparedness planning, not for sustained preparedness assessments.

39. *NPR* 2012, 3.

40. *NPR* 2012, 1. A unique challenge faced by the first *NPR* was handling the transition from *HSPD-8* to *PPD-8,* which entailed working with the new set of thirty-one *PPD-8* core capabilities while facilitating a transition from the

old to the new system. This complicated efforts to identify measurable performance and assessment data to determine annual yearly progress in implementing. Given the press of time to get the first *NPR* out the door, the FEMA team was forced to assess the county's overall preparedness progress by utilizing existing assessment approaches and associated data based on the *old* capabilities and targets associated with *HSPD-8,* not the *new PDD-8* core capabilities and their associated performance targets. For this and other reasons, this first *NPR* candidly acknowledges that "the rating system used to score target capability goal performance on a scale of 100% is not reliable and…in many cases, measures and metrics do not yet exist to gauge performance […for use as] a reliable source of deficiencies nor for that matter of successes." *NPR* 2012, 60.

41. As articulated in the 2013 NPR, " trends in national preparedness will be increasingly evident in future reports, as the *NPR* development process continues to mature and incorporates additional input from across the whole community [… and] more significant changes in levels of capability and overall national preparedness will become clearer by evaluating trends across multiple years." *NPR* 2013, 1.

42. *NPR* 2013, 12.

43. The intent of an early test program, held in 2006, was to learn important lessons about real implementation challenges for *HSPD-8* and significantly revise the methodology for further use in measuring the preparedness level of States. Working with FEMA, six States conducted Pilot Capability Assessments (PCAs). Each PCA was subjected to a self-assessment, with inputs from a selected number of SSRs in each State. All this effort led to uneven, inconsistent, and not analytically based outcomes. Many difficulties arose in implementation and funding. Some believe that this program represented a good start, but it faded away. See U.S. Department of Homeland Security, Preparedness Directorate, Office of Grants and Training, *Pilot Capabilities Assessment (PCA): RDSTF Region 3*, September 15, 2006, and *RDSTF Region 7*, July 17, 2006. See also FEMA, "Measuring Effectiveness – Capabilities Assessment," http://fema.ideascale.com/a/dtd/Measuring-Effectiveness-Capabilities-Assessment/316114-14692 Further complicating this process is the continued growth of intra and cross state regional cooperation on homeland security. This has led to an evolving structure of layered and often overlapping cooperative arrangements at various levels across the nation, reflecting different purposes and defined through various organizing principles. How to account for these arrangements in developing intra state and regional risk assessments without facing such issues as double counting and merging differing methodologies is quite demanding.

44. *FEMA Has Made Progress,* GAO-13-637, June 25, 2013.

45. See Ozzie Mascarenhas, "Innovation as Defining and Resolving Wicked Problems," http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCcQFjAA&url=http%3A%2F%2Fweaverjm.faculty.udmercy.edu%2FMascarenhasLectureNotes%2FMascarenhasWickedproblems.doc&ei=Rv_zUq71DsPdoAS2yIGIBg&usg=AFQjCNFa8lMBrjeiuoUfsnY6i1vsHR_TZA&sig2=U95veKrqyfn4nJpj-1qebw May 11, 2009 at On Wicked Problems and their Solution Strategies. For the homeland security context, see Jay Rosen, "What Are Journalists For?" PressThink.org, 2005.

46. *FEMA Has Made Progress, but Additional Steps Are Needed to Improve Grant Management and Assess Capabilities,* Government Accountability Office, GAO-13-637 (June 25, 2013), 1, at http://www.gao.gov/products/GAO-13-637T

47. *Assessing National Preparedness: Integrating and Aggregating Capability Assessments*, Homeland Security Studies and Analysis Institute (HSSAI), Final Report, 28 March 2007, Prepared for the Department of Homeland Security (DHS), Preparedness Directorate, for the National Preparedness Task Force. At the moment, the HSSAI document remains designated For Official Use Only (FOUO), meaning it contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 522). For this reason, it must be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information, and not to be released to the public or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. Contact author for suggestions on how access might be obtained.

48. Assessing national preparedness might use a form of network analysis, but this method has apparently not been developed for this purpose. See Andrew Gelman, "Multilevel Hierarchical Modeling: what it can and can't do" (June 1, 2005), 1, http://www.cs.berkeley.edu/~russell/classes/cs294/f05/papers/gelman-2005.pdf; *No Child Left Behind: A Roadmap for State Implementation* (Washington, DC: November 10, 2005), http://www2.ed.gov/admins/lead/account/roadmap/roadmap.pdf.

49. *The Goal*, 3.

50. To the author, *PPD-8* wins the complexity battle. For example, *PPD-8* adds a fifth mission of mitigation to the four used in *HSPD-8*, provides a risk methodology for stakeholders to adapt and apply that is not done in *HSPD-8*; focuses on a National Preparedness System with Planning Frameworks playing a prominent role unlike HSPD-9, and calls for annual national-level progress reports that have no formal counterpart in *HSPD-8*.

51. Corey Gruber, at that time Director of the DHS Office of Grants and Training, cited in Sharon Caudle, "Homeland Security and Capabilities-Based Planning: Improving National Preparedness," (master's thesis, Naval Postgraduate School, September 2005), 33.

52. Christopher Bellavita, *Homeland Security Watch,* Preparedness and Response, April 12, 2011, www.hlswatch.com/2011/04/page/2/. For analyses of federalism as it relates to homeland security, see Pietro S. Nivola, "Reflections on Homeland Security and American Federalism," *The Brookings Institution* (Working Paper), May 13, 2002 and Samuel H. Clovis Jr. "Federalism, Homeland Security and National Preparedness: A Case Study in the Development of Public Policy," *Homeland Security Affairs* 2, no. 3 (October 2006).

53. What the President does *not* need is a repeat of the way *ObamaCare* was advertized, where the whole story was not made public at the beginning of public rollout – i.e., "if you like your plan, you can keep it!"

54. Among the many ongoing outreach efforts is the idea of National Preparedness Months, where FEMA provides tool kits with "suggestions" for activities and events that state, local, tribal and territorial governments, business, non-governmental organizations, and community organizations could sponsor to promote the initiative. Toolkits also include templates and drafts of newsletter articles, blogs, posters, and other collateral material that local as well as state and federal organizations can use y in various outreach efforts.

55. One effort along these lines is a pilot, voluntary certification program that aims to make homes and buildings more secure and resilient to all hazards. Homes that receive a Resilience STAR™ designation will be awarded one to five stars, five being the highest level of capabilities attained. See Secretary Janet Napolitano before a Senate Committee on the Judiciary hearing, "The Oversight of the Department of Homeland Security," April 25, 2012. See also Homeland Security News Wire, August 20, 2013. This is consistent with PPD-8 calling for "private-sector programs to enhance national resilience." *PPD-8,* 3.

56. One aspect of *PPD-8*'s attempt to engage stakeholders is its calls for a comprehensive campaign to build and sustain national preparedness. As part of this overall effort, the administration developed a public outreach and feedback program called the *Campaign to Build and Sustain Preparedness*. FEMA also established a website to facilitate interaction with the public in terms of progress made and suggestions from stakeholders regarding content and implementation of *PPD-8*. There are limits, however, as to how effective this outreach and feedback program can be in helping stakeholders and the public understand, accept, and execute the *PPD-8* plans. In principle, a more "hands on" approach with FEMA officials interacting on a sustained basis with community leaders, non-governmental organizations, businesses, and interested citizens has greater potential to have a significant impact. In practice, however, this would require a costly increase in developing a well-trained and large enough outreach force, which is likely to prove prohibitive.

57. For example, DHS could ask the Homeland Security Studies and Analysis Institute (HSSAI), its Federally Funded Research and Development Center (FFRDC), to conduct such an assessment, consistent with its charter. It would be beneficial if independent reviews could also be done for each of the *SSR* assessments and each of the sub-state inputs to the State reports, but these may simply not be practical, especially the latter.

58. The sum of all these individual *PPD-8* products might, if printed and stacked, compete in size with the hard copy set of the Encyclopedia Britannica volumes some readers may still have adorning their bookshelves.

59. The kit would also contain links to an available database of estimated likelihoods and consequences for different hazards in connection with different types and sizes of communities, urban areas, regions as well as businesses, and other entities. Also part of the kit would be a National Planning System Guide for creating and maintaining the Frameworks and operational plans required to make all parts of the overall *NPS* work for all users—an effort that is supposed to be underway if not yet completed. www.fema.gov/pdf/prepared/nps_description.pdf. The last part of the kit, perhaps in an appendix, would demonstrate how results could be horizontally integrated and vertically aggregated to get a national level assessment by mission, capability, and stakeholder type (along the lines of the limited access HSSAI report, which could be officially approved for public release, assuming FEMA takes this initiative.

60. Recall such issues as publishing a *TCL* that includes only half of the core capabilities identified and neglecting to provide stakeholders with risk assessment guidelines.

61. Some might see the Obama *PPD-8* initiative as largely a repeat of *HSPD-8* with few changes that matter. Others might see *PPD-8* as having more elements and adding more layers of detail than *HSPD-8*. Still others might hold the view that *PPD- 8* seems to be "a modest evolution of *HSPD 8*, with more attention to a broader set of stakeholders, and with at least the hint of more flexibility about what preparedness means"....Christopher Bellavita, Homeland Security Watch, "Preparedness and Response" (April 12, 2011) http://www.hlswatch.com/2011/04/12/there-is-a-quality-even-meaner-than-outright-ugliness/ See also Philip J. Palin, "PPD-8 as a natural evolution of HSPD-8: Preparedness and Response," Homeland Security Watch, April 9, 2011, and Jared Brown, *Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress,* CRS Report (Washington D.C, October 21, 2011).Past experience does not always govern future performance. If the earlier *HSPD-8 e*xperience did not work well, however, useful lessons can be learned on what not to do, but not necessarily on how to solve problems the second time around.

62. *The Goal,* 1.

63. This saying, originally with its three "tries," was popularized by educator Edward Hickson (1803-70) in his *Moral Song*. It is now applicable in any of its forms, to all activities, not just educational. *Oxford Dictionary of Proverbs* (New York: Random House, 1996), 154.

# Hybrid Targeted Violence:
## Challenging Conventional "Active Shooter" Response Strategies

Tracy L. Frazzano and G. Matthew Snyder

**ABSTRACT:**

*Hybrid Targeted Violence (HTV) is defined as an intentional use of force to cause physical injury or death to a specifically identified population using multifaceted conventional weapons and tactics. This article introduces the HTV concept to challenge first responders to prepare for violent "hybrid" multi-threat incidents. These incidents may involve conventional weapons, the use of fire as a weapon, chemical weapons, and/or improvised explosives. Attacks of this nature defy conventional thinking about the role of police, fire, and emergency medical professionals. HTV events demand cooperative strategies to efficiently neutralize complex threats that are beyond the capacity of a single first responder discipline. Recent and historical HTV incidents are identified to reinforce the compelling need for a paradigm shift in thinking that goes beyond conventional "active shooter" scenarios that do not advance "Whole Community" interdependent response strategies.*

## INTRODUCTION

Mass casualty attacks in the United States immediately capture the attention of the nation. These horrific and calculated acts garner international media attention due to the compelling questions of "why" and "how" such an atrocity could occur. While mass murder rampages in non-combatant environments are perceived by many to be a modern phenomenon, they are neither new nor are they growing at epidemic rates. Despite the low frequency of these events, they dramatically impact countless individuals, communities, and nations by instilling fear that such events can unpredictably occur in urban, suburban and metropolitan areas. The recent Nairobi Westgate Mall Attack, the Washington Navy Yard shooting, and the protracted Boston Marathon bombing and subsequent violence all underscore the diversity of the communities impacted by targeted violence.

Events involving sophisticated planning, varieties of weapons, and complex tactics will undoubtedly persist globally in highly unpredictable patterns. International political attention and intense media coverage of mass casualty attacks in Africa, South Asia, and the United States have led domestic public safety professionals to consider mitigation, response, and recovery strategies for these low-frequency high-risk terror driven events.[1] The high profile lethality of these seemingly senseless acts of violence has raised the public's expectation that first responders be poised to rapidly and skillfully protect potential victims in areas that have minimal protection, such as schools, houses of worship, workplaces, and public gathering venues.

The current Department of Homeland Security definition of an active shooter is "an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearm(s) and there is no pattern or method to their selection of victims."[2] That definition does not adequately describe for first responders or the public the dynamic crime scenes that may involve a variety of lethal weapons and mobile attackers, and are not restricted to a singular location. The active shooter label is no longer sufficient to accurately describe the enhanced threats that public safety will certainly be called upon to resolve. The active shooter label also does not provide a sufficiently descriptive term to comprehend the broad range of weapons and tactics that may be used in an act of targeted violence.

Influencing changes in thinking, training, and tactics requires a more explanatory term to describe these complex threats. Hybrid Targeted Violence (HTV) has been defined as an

intentional use of force to cause physical injury or death to a specifically identified population using multifaceted conventional weapons and tactics.[3] We suggest this definition, based on "hybrid" weapons and tactics, better captures the operational range of hazards confronting first responders and the communities they serve.

HTV assaults often use a combination of lethal conventional weapons (i.e. fire as a weapon, firearms, improvised explosive devices, chemical weapons, etc.) and a combination of well-planned tactics (i.e. ambush, breaching, barricading, maneuver, etc.). (See figure 1). The compound effect of this form of violence requires a more synergistic response strategy. Research associated with integrated responses to school violence has found significant inadequacies in training and interagency communication.[4] Effective HTV response strategies blur lines between traditional law enforcement, fire, and emergency medical service duties and responsibilities. A common and cooperative operating picture must drive first responder decision making at chaotic HTV events. All responders must be principally focused on threat elimination and lethality reduction. This cooperative level of response can only be achieved through pre-event dialogue, planning, and joint public safety discipline HTV exercises.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| (Multiple Weapons) | + | (Targeted Population) | + | (Planned Violent Action) | = | HTV |
| Example: | | | | | | | |
| (Small Arms) | + | (School Population) | + | (Ambush Tactics) | = | HTV |

**Figure 1:** Hybrid Targeted Violence formula and example.

Targeted violence directed towards innocent and defenseless people, especially children, demands a highly competent, rational reaction. Professionals must extract lessons from past events to better prevent, disrupt, and mitigate future attacks. The reality of confronting an armed attacker who has employed fire or explosives to actively kill people confounds the traditional roles that define which first responders engage a threat and which first responders stage until the scene is secure. The lack of engagement due to awaiting scene security by law enforcement and the cost associated with delayed Fire and Emergency Medical Services engagement was clearly documented in the Rand Corporation's *Lessons on Mumbai* report.[5] Future HTV incidents require first responders to engage as members of the same team, not members of role-defined public safety disciplines, to save lives and neutralize a no-notice rapidly lethal attack.

## LEVERAGING LESSONS OF THE PAST

Preparation for future HTV events requires an appreciation for historical incidents while maintaining a keen awareness for impending threats. Past events that have involved combinations of ambush strategies, explosive devices, firearms, and other targeted assault tactics are relevant educational resources. First responders have the opportunity to glean valuable training lessons from these events by comparing local resources against actual HTV tactics. Introspective assessments involving all first responder disciplines are likely to reveal collective strengths and individual weaknesses.

Following the Sandy Hook Elementary School Attack and the Aurora Colorado Theater Ambush, the New York Police Department published a revised active shooter risk mitigation report.[6] The NYPD's report provides a global analysis of HTV incidents with sufficient detail to permit further research involving primary reference sources. A worldwide frame of

reference is beneficial when studying both HTV tactics and HTV response strategies by first responders in non-combatant environments.

Examples of noteworthy attacks that can serve as the basis of first responder HTV awareness and training include:

- May 18, 1927: Bath Township Michigan School Massacre: Ambush, bombing, fire as weapon, and shooting.[7]
- December 30, 1974: Olean New York High School Attack: Ambush, bombing, fire as weapon, and shooting.[8]
- April 20, 1999: Columbine Colorado High School Attack: Ambush, fire as weapon, IED's, and shooting.[9]
- December 9, 2003: Visalia California PrintXcel Plant Attack: Multiple fires as weapons and shooting.[10]
- November 26, 2008: Mumbai India Coordinated Attacks: Ambush, barricading tactics, explosives, fire as weapon, military maneuver tactics, and shooting.[11]
- August 27, 2010: McKinney Texas Department of Public Safety Ambush: Ambush, fire as weapon, and shooting.[12]
- July 22, 2011: Oslo Norway Parliament and Children's Camp Attack: Ambush, distraction vehicle borne improvised explosive device (VBIED), maneuver techniques, and shooting.[13]
- December 13, 2011: Liege, Belgium Saint-Lambert Attack: Ambush, shooting, and stun grenades.[14]
- July 20, 2012: Aurora Colorado Theater Attack: Ambush, chemical weapons, explosive booby traps and shooting.[15]
- December 14, 2012: Sandy Hook Elementary School Attack: Ambush, breaching tactics, and shooting.[16]
- December 24, 2012: Webster New York Firefighter Ambush: Ambush, fire as weapon, and shooting.[17]
- April 15-21, 2013: Boston Marathon Bombing and Suspect Pursuit: Ambush, improvised explosive devices (pressure cooker bombs), and shooting.[18]
- September 16, 2013: Washington Navy Yard Shooting: Ambush and shooting.[19]
- September 21-23, 2013: Westgate Shopping Centre Attack in Nairobi, Kenya: Ambush: barricading tactics, explosives, fire as weapon, military maneuver tactics, and shooting.[20]

The Federal Bureau of Investigation (FBI) and United States Secret Service (USSS) are engaged in ongoing efforts to catalog and analyze events involving mass casualties and violence targeted at specific populations, such as schools. An advisory published in December of 2012 by the Department of Homeland Security and the FBI calls for increased vigilance and coordinated response plans across functional disciplines based on the study of over 100 multi-victim attacks between 2000 and 2012.[21] The USSS remains an authority on school campus related violence. The USSS led study, "Campus Attacks: Targeted Violence Affecting Institutions of Higher Education," provides both historical and visionary perspectives on "soft target" environments for no-notice violence.[22] Artifacts from past HTV incidents and empirical analysis of HTV trends are readily available to facilitate the improvement of public safety community response capabilities.

Incidents of hybrid targeted violence and less sophisticated targeted violence have achieved high levels of lethality in both domestic and international venues. Federal, state, local, and tribal government officials are embracing the reality that these threats may present. With little to no notice, individual responders must have well-crafted strategies to cooperatively address active threats involving firearms, improvised explosives, fire as a weapon, and military style barricading and maneuvering techniques. The well-documented and studied history of these events are worthy of ongoing study to shape future response strategies.

## COLLECTIVE PARADIGM SHIFT

Executive and operational leaders need to make the transition from analyzing historical HTV lessons to planning for future HTV attacks with local resources. These leaders must remain cognizant of the fact that HTV events occur with little or no notice; therefore, realistic strategies and resourcing expectations should be established. The Federal Emergency Management Agency (FEMA) utilizes a "Whole Community" approach, engaging with members of the community as collaborative resources to enhance the resiliency and security of our nation. This engagement is necessary to relieve first responders of the restrictions associated with traditional "stage until the scene is secured" ideologies that are insufficient for no notice high-risk violent events.

There is considerable confusion and chaos at the start of HTV events, so much that the initial first responders rely heavily on training and past experiences to recognize and react to the atypical threats. The problem is that effective HTV responses involve multiple disciplines working collectively yet most public safety disciplines (police, fire, EMS, etc.) historically train in isolation from one another. Executive and line level first responders should be engaged in collaborative pre-event "if-then" dialogues. These conversations and tabletop exercises can benefit from no-notice scenarios that involve known casualties, the immediate threat of additional casualties, fire being used as a weapon, and uncontained armed attackers. These scenarios will demand a coordinated response from police, fire, and emergency medical services leveraging sound tactical protocols to address dynamic threats.

What is evident in all of these scenarios is a need for change in the traditional roles of each organization dispatched to a HTV event. The public, the media, and even first responders look to the law enforcement community alone to manage incidents involving violent criminal conduct. Television coverage amplifies the visual of police and SWAT officers running to the scene wearing body armor and carrying tactical firearms. Initial images of the Columbine and Virginia Tech school shootings portrayed the fire department and emergency medical community in the "staging" area awaiting the police to deem the area safe or bring patients to them. The operational and technical resources that these "staged" disciplines bring to a HTV scene should be immediately utilized in a manner that capitalizes on their capacities in order to extinguish the threat an attacker presents to civilians and responders. Balancing first responder safety against taking life-saving action is a critical piece of calculus that warrants an assessment of tactical and logistical capabilities against HTV hazards.

A collective paradigm shift in first responder perspectives and cultures is necessary to better address hybrid threats and targeted violence. Discipline-centered basic and advanced training has not fostered a spirit of dynamic cooperation at crime scenes or on the fire ground. For example, police officers are trained to address acts of violence, firefighters are trained to fight structure fires, and EMT's are trained to care for the injured. These fundamental roles are not realistically applicable during a HTV event.

When roles overlap, leaders across disciplines must question the methods of interoperability. For example, under the current model, can police officers, firefighters, and EMT's simultaneously engage an active shooter within a burning building when lethal injuries are being inflicted every few seconds? Hard questions must be addressed with an honest self-assessment. Introspective organizational self-assessments should ideally occur before a HTV crisis is experienced. A culture of interdependence and resource sharing must be stimulated in a training environment in order to be inculcated in an operational environment.

## TRAINING

During a HTV event, first responders are making split-second decisions involving tasks and responsibilities outside their traditional response domain, and therefore outside their general areas of expertise. It is commonly accepted that under stress, most responders will revert to what they have been trained to do. While it is easy to criticize the choices made during an event, making instantaneous

decisions is a difficult task in which instincts, prior training, and knowledge come into play. Each discipline commonly derives lessons learned and future response strategies from actual attacks and complex disasters that have occurred in the past. Thoughtful operational research has the potential to inform and educate those who may be called to respond to the next Aurora Theater Attack, Boston Marathon Bombing, or Nairobi Westgate Mall Attack.

One of the most recognizable paradigm shifts in law enforcement tactics occurred after the Columbine High School shooting in 1999. According to the Columbine Review Commission, during the forty-six-minute rampage, "no efforts were made [by law enforcement] to engage, contain, or capture the perpetrators"[23] Based on the findings of the report, law enforcement policy and training now emphasize that the highest priority of arriving law enforcement officers is to rapidly stop any ongoing assault. During this same incident, fire and emergency medical service resources were staged away from the hot scene due to protocols in place at the time. This "stage until safe" approach resulted in 3½ hours passing until the last wounded survivor was removed from the school for medical care. In the years following this incident law enforcement has adopted instrumental changes in their response tactics. Unfortunately, other functional disciplines of first responders, such as fire and emergency medical services have not universally changed their tactics in the face of uncontained lethal forces. Respected organizations such as the United States Fire Administration have recognized the need to alter conventional response strategies through practitioner developed operational guidelines for active shooter and mass casualty events with the understanding that such HTV events may be well beyond the traditional training and experience of the majority of firefighters and emergency medical technicians.[24]

Paradigm shifts in public safety tactics are most effective when a collective change occurs across all functional disciplines. The aforementioned delay in treatment by fire and EMS personnel during incidents such as the Columbine shooting is an area that warrants constructive analysis. Conventional doctrine holds that every functional discipline has saving lives as their primary role. Integrated training involving all disciplines will benefit the collective desire to save lives in the face of the full continuum of lethal violence targeted at defenseless populations. Police, fire, and emergency medical disciplines will collectively benefit from critical conversations that yield innovative solutions to HTV events. These conversations should occur regularly and be part of a deep seeded inculcation strategy rather than a single joint exercise that yields minimal long-term benefits.

There are examples of fire and emergency medical services engaging in collaborative HTV response strategies. In 1999, the Columbine High School massacre triggered change in the Arlington County Fire Department (Virginia). In conjunction with the Arlington County Police Department, a fortified and trained group of tactical medics known as the Rescue Task Force (RTF) was established. The RTF approach to law enforcement and emergency medical service integration utilizes police as cover for medics for entry within a "warm zone" to treat injured victims with live saving tactics that have proven effective when used by the military in wartime environments.[25] The RTF concept has evolved over the years and it remains a highly desirable multidisciplinary response model for other jurisdictions to study and adopt.

First responders in Arlington County have embraced the difficult but necessary process of redefining their cultural and operational identities. The training and tactics that these professionals receive enhances their ability to coordinate, cooperate, resolve, contain, and mitigate the effects of a HTV. Rather than use the reality of constricting budgets as an excuse not to make the needed changes, Arlington County has recognized that building cooperative emergency service teams leads to a more economical and effective life saving force.

Development of an interdisciplinary response mindset is the essential first step. This mindset should be reflected in written plans and agreements, reinforced through regular meetings, and practiced during exercises and actual emergencies.[26] This collective versus

functional mindset requires a collaborative transition process and a significant change to each of the police, fire, and EMS cultures. According to a study by Stinchcomb and Ordaz on the merger of police and fire into one organization, "because the influence of culture tends to exceed the regulatory capacity of conventional policies and procedures, it can become a significant make-or-break factor in achieving organizational change."[27] It is important to note that the historical and cultural artifacts of each emergency service discipline are not discarded; instead each group maintains their rich history but with a new outlook that recognizes the practical utility of dynamic collaboration.

While the event in Columbine triggered a profound change in police response, it has had less of an impact in the fire and emergency medical communities. Best practices for collaboration, such as those employed in Arlington, Virginia should serve as an example to prepare other communities to address HTV events. Effective training programs and response protocols take years to develop and usually are derived from a tragic event. Unfortunately, this means that many public safety professionals are training for past events rather than taking steps to deter future ones. The *9/11 Commission Report* underscored the inherent risk of permitting a "failure of imagination" to prepare for future threats – such as a HTV event. First responders must not fall prey to failures of imagination or parochial response strategies when faced with an HTV event. Minimizing the effect and lethality of an attacker will require rapid Whole of Community responders working as one team rather than a series of domain specific teams. The first responder profession involves a continual learning experience because those who want to do harm to the world are forever finding new ways to accomplish their missions.

## WHOLE COMMUNITY

Whole Community suggests that shared understanding of community risks, needs, and capabilities leads to an increase in resources through the empowerment of community members.[28] While specifically used to address national disasters, the approach is not a new concept. Sir Robert Peel, the founder of modern policing, established "principles of policing" when he organized the London Metropolitan Police Service in 1829. Peel's principles focused on the constabulary's dependent relationship with the community. Peel recognized that willing cooperation by the public with the police should be actively cultivated at all times. The private sector is an integral component of the whole community when it comes to a HTV event. This influential sector provides a diversity and breadth of assets and capabilities that are not fully recognized by the first responder community. By utilizing the private sector, first responders develop a "megacommunity" of organizations whose leaders and members have deliberately come together to achieve goals that could not and have not been achieved alone. Due to their fiscal and political exposure, private entities are vital stakeholders in the Whole Community model that is impacted by manmade disasters that include the types of HTV attacks experienced recently in Boston and Nairobi.

## SUMMARY

Effective responses to HTV events hinge on integrated public safety professionals applying finely tuned skills to perform essential tasks cooperatively in a lethal multi-hazards environment. Joint planning, training, and understanding across disciplines are required to more efficiently neutralize chaos and confusion during the initial response to a HTV incident scene. The men and women on duty at the time of a HTV event must be an empowered and educated first line of defense. Multi-discipline Quick Reaction Forces of line level personnel will be called upon to confront armed adversaries, fight fires, breach barricades, and negotiate explosive traps all while trying to rescue the survivors and treat the wounded.

The first few minutes of any emergency call for service are the most lethal for both innocent victims and first responders. It is common for both groups to be the initial targets of a HTV attack. Quick identification and recognition of a HTV incident expedites the process

through which first responders request and receive the appropriate resources to engage the threat. Minimizing the damage inflicted by a determined attacker can pivot on a rapid recognition by all responders that a call for service is not a routine gun call, structure fire, or medical request.

The concept behind the term "Hybrid Targeted Violence" is intended to foster a collective change in mind-set to all first responder disciplines. Achieving that change through multi-discipline training and education will shorten the reaction time between attack initiation and neutralization through a Whole Community response.[29] Creative strategies, such as the insertion of a deliberately set fire in an active shooter training scenario can facilitate higher levels of preparedness with minimal impact on finite training budgets. The reality of a complex conventional weapons attack (i.e., Mumbai 2008) occurring again, especially in the United States, must be contemplated when developing resilience strategies.[30]

When lives are being lost to a HTV attacker during those initial few seconds, first responders must be capable of abandoning routine response strategies and adopting synergistic strategies. This paradigm shift will maximize lifesaving forces in the face of danger that is seemingly unimaginable. Ready, resilient, and resourced collectives of interoperable first responders are needed to effectively engage and counter the unpredictable events that occur during a Hybrid Targeted Violence incident.

## ABOUT THE AUTHORS

***Tracy L. Frazzano*** *is a Lieutenant with the Montclair Police Department in New Jersey. She serves as a subject matter expert and instructor for the National Center for Security & Preparedness supporting the New York State Division of Homeland Security and Emergency Services. Lieutenant Frazzano was awarded the 2011 Center for Homeland Defense and Security Alumni Fellowship and was detailed to the United States Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) in Washington, DC for one year. A 2010 graduate of the Center at the Naval Postgraduate School in Monterey, California, she earned a Master of Arts Degree in Security Studies (Homeland Security and Defense). She also has a Master of Arts Degree in Human Resources Training and Development from Seton Hall University. Contact: tfrazzano@gmail.org.*

***G. Matthew Snyder*** *is an advanced leadership instructor with the Department of Homeland Security (U.S. Customs and Border Protection) Advanced Training Center in Harpers Ferry, West Virginia. He has been employed as a police officer with the City of Waynesboro (VA) Police Department since 1992. Formerly a full time patrol officer, he now serves as a part-time investigator assigned to the Criminal Investigations Division. In 2010, Mr. Snyder retired from the U.S. Army at the rank of Command Sergeant Major with over twenty-four years of active and reserve service. He earned a Master's Degree in Public Administration from James Madison University and he recently completed all coursework towards a Doctorate in Education at Liberty University. His ongoing dissertation research is focused on training and education related to hybrid targeted violence and active shooter events. Contact: gmatthewsnyder@gmail.com.*

## NOTES

1. Todd Bates, "U.S. malls vigilant in wake of Kenyan assault," *USA Today*, September 25, 2013, retrieved from http://www.usatoday.com/story/news/nation/2013/09/25/mall-security-kenya-siege/2868887/; D. Simpson, "Kenya-style mall attack: Can it happen here? Smaller plots have been thwarted," Cable News Network, September 23, 2013, http://www.kxlh.com/news/kenya-style-mall-attack-can-it-happen-here-smaller-plots-have-been-thwarted/

2. Department of Homeland Security, *Active Shooter: How to Respond* (Washington, DC: DHS, 2008), http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf

3. T.L. Frazzano and G.M. Snyder, "Hybrid Targeted Violence: Clearly Defining Complex Attacks," Homeland Security Watch, February 12, 2013, http://www.hlswatch.com/2013/02/12/hybrid-targeted-violence-clearly-defining-complex-attacks/.

4. D.W. Callaway, T.C. Westmoreland, A.A. Baez, S.A. McKay, and A.S. Raja, "Integrated response to the dynamic threat of school violence," *Prehospital Disaster Medicine* 25, no. 5 (2010): 464–470.

5. A. Rabasa, R.D. Blackwill, P. Chalk, et. al, *Lessons on Mumbai* (Santa Monica, CA: Rand Corporation, 2009).

6. Counterterrorism Bureau of the New York City Police Department, *Active Shooter: Recommendations and Analysis for Risk Mitigation* (New York: New York City Police Department, 2012), http://www.nyc.gov/html/nypd/downloads/pdf/counterterrorism/ActiveShooter2012Edition.pdf.

7. S. Bomboy, S. (2012, December 18). "Huge school bombing in 1927 puts Sandy Hook in context," Yahoo!News, December 18, 2012, http://news.yahoo.com/mass-school-bombing-1927-puts-sandy-hook-context-185608674.html.

8. NYPD, *Active Shooter,* 143.

9. Ibid., 121.

10. Ibid., 83.

11. Ibid., 50.

12. Ibid., 13-14.

13. Ibid., 175.

14. Ibid., 34.

15. Ibid. 33.

16. Callaway, et al., "Integrated response"; NYPD, *Active Shooter,* 91.

17. C.E. Shoichet and G. Botelho, "'Chaos:' Gunman ambushes, kills two firefighters at New York blaze" Cable News Network, December 24, 2012, http://www.cnn.com/2012/12/24/us/new-york-firefighters-shooting/index.html.

18. Federal Bureau of Investigation (FBI), "Updates on Investigation into Multiple Explosions in Boston," October 21, 2013, http://www.fbi.gov/news/updates-on-investigation-into-multiple-explosions-in-boston

19. Federal Bureau of Investigation (FBI), "Law Enforcement Shares Findings of the Investigation into the Washington Navy Yard Shootings," September 25, 2013, http://www.fbi.gov/washingtondc/press-releases/2013/law-enforcement-shares-findings-of-the-investigation-into-the-washington-navy-yard-shootings.

20. British Broadcasting Corporation," Nairobi siege: How the attack happened, BBC News Africa, October 18, 2013, http://www.bbc.co.uk/news/world-africa-24189116.

21. FBI/DHS bulletins are distributed through public safety venues as "official use only" resources.

22. D.A. Drysdale, W. Modzeleski, and A.B. Simons, *Campus Attacks: Targeted Violence Affecting Institutions of Higher Education* (Washington, DC: U.S. Secret Service, U.S. Department of Education, Federal Bureau of Investigation, April 2010) http://www.fbi.gov/stats-services/publications/campus-attacks.

23. William H. Erikson, *The Report of Governor Bill Owen's Columbine Review Commission* (Denver, CO: State of Colorado, May 2001), http://www.state.co.us/columbine/Columbine_20Report_WEB.pdf

24. U.S. Fire Administration, *Fire/Emergency Medical Services Department Operational Considerations and Guide for Active Shooter and Mass Casualty Events* (September 2013), http://www.usfa.fema.gov/fireservice/ops_tactics/disasters/.

25. E.R. Smith, B. Iselin, and S. McKay, "Toward the Sound of Shooting," JEMS Journal of Emergency Medical Services (December 2009); 34(12):48-55.

26. U.S. Fire Administration, *Operational Considerations and Guide.*

27. J.B. Stinchcomb and F. Ordaz, "The Integration of Two "Brotherhoods" into One Organizational Culture: A Psycho-social Perspective on Merging Police and Fire Services," *Public Organization Review* 7, no. 2 (2007): 143-161.

28. Federal Emergency Management Agency (FEMA), *A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action* (Washington, DC: FEMA, 2011), http://www.fema.gov/library/viewRecord.do?id=4941.

29. T.L. Frazzano, (2010). Local jurisdictions and active shooters: building networks, building capacities. *Naval Post Graduate School, Center for Homeland Security Studies*. Monterey, CA.

30. R.S. Mueller, III, "Remarks prepared for delivery, Director, Federal Bureau of Investigation," *Council on Foreign Relations*, February 3, 2009, http://i.cfr.org/intelligence/prepared-remarks-conversation-robert-s-mueller-iii/p18594

# EMS and Homeland Security

Mac Kemp

## ABSTRACT

*Emergency Medical Services (EMS) is a vital partner in everyday emergency response and in homeland security. To date EMS has not been included in most homeland security activities and EMS needs to expand its role in this enterprise. EMS should play a greater role in disaster response, recovery, intelligence gathering, fusion centers, and syndromic surveillance. EMS could increase its value in homeland security and make real contributions with some additional training and protocols.*

## INTRODUCTION

Emergency Medical Services (EMS) plays a vital role in the United States in responding to medical emergencies and transporting patients. While a relatively young profession, EMS, with law enforcement and the fire service, constitute one third of the routine 911 emergency response system. The out-of-hospital treatment and transport of patients, a function performed by EMS, is a primary function required at almost every disaster. While the response-phase contribution of EMS is understood, EMS has can make significant, unique, critically important contributions to the prevention, mitigation, and recovery phases of the homeland security cycle.

EMS personnel can be trained to function as intelligence sensors to identify suspicious indicators of terrorism and to report those indicators to intelligence fusion centers. EMS personnel can also provide medical intelligence within fusion centers to help those centers better understand the significance of clinically related tips, leads, and indicators. EMS personnel can also develop and disseminate medical intelligence briefs, which inform EMS, fire, law and other responders of medically based threats to their health and safety. This is an important component of comprehensive force protection and has been used by the United States and foreign military for decades. EMS must lead development of multi-disciplinary mass casualty response plans and other emergency medical related planning and exercising. At the county, regional, or state level, EMS must form networks of ambulance strike teams to respond to areas devastated by catastrophic events. Finally, EMS data can be used to augment and enhance current syndromic surveillance systems to provide earlier warning of a pandemic or terrorist incident.

### Background

EMS has existed in its modern form since the early 1970s. It is a young and dynamic profession. While most people recognize EMS as a fire engine or ambulance responding to an emergency call, EMS also includes using paramedics to provide support to primary medical care in communities, and transporting ill or injured patients between medical facilities. EMS is provided by municipal and county-based providers, fire based systems, private providers, and hospital based systems. EMS personnel are paid and volunteer. These various delivery systems have complicated the maturation of EMS, because each delivery system has a slightly different perspective of the optimal EMS system; some have adapted EMS to better suit their core mission. These divisions have resulted in inconsistent lobbying efforts at local, state, and federal levels.[1] As a consequence, the federal government has not designated a lead agency for EMS, set standards for EMS performance in the homeland security mission, provided adequate funding to EMS (less than 4 percent of HHS and DHS grant funding has been dedicated to EMS), nor provided adequate homeland security related training for EMS personnel.[2]

## The Core Mission of EMS

Most EMS agencies and personnel are very clear about what their core mission is from day to day. Even with a diverse set of agencies providing EMS services, what is provided falls within a fairly recognizable scope. EMS responds to, treats, and transports patients who are ill and injured. EMS occasionally responds to mass casualty incidents and also occasionally to unusual calls such as hazardous materials. EMS also provides ground and air transport over long distances and generally provides a form of social services in the field when no other agencies are indicated or available. This common ground could be the basis of forming a cohesive scope of practice within homeland security that could be applied to all EMS agencies regardless of what delivery model is used. Delivery methods of EMS vary mainly because local needs are different; however a universal approach to homeland security issues could easily be applied to all of the divergent agencies to create a powerful extension of the homeland security enterprise. According to Michael Petrie, Director and Chief of EMS for Santa Clara County, California, a jurisdiction of 2.1 million people, "EMS plays a pivotal role in response roles in homeland security now, but it is also critical that EMS plays a role in prevention."[3]

## EMS Homeland Security Roles

According to the *National EMS Assessment* of 2011, there are currently over 900,000 EMS personnel in the United States.[4] This large and highly skilled workforce can significantly and materially improve local, state, and federal government's performance in planning for, response to, mitigation of, and recovery from homeland security and disaster events. Specifically, EMS can be an integral part of homeland security through the following five programs:

1. EMS personnel should be trained to function as intelligence sensors to identify suspicious indicators of terrorism and to report those indicators to intelligence fusion centers.
2. EMS personnel should provide medical intelligence within fusion centers to help those centers analyze medical data that could provide indicators of potential threats.
3. EMS personnel should develop and disseminate medical intelligence briefs, which inform EMS, fire, law and other responders of medically based threats to their health and safety.
4. EMS must lead development of multi-disciplinary mass casualty response plans and other emergency medical-related planning and exercising, including networks of ambulance strike teams to respond to areas devastated by catastrophic events.
5. EMS data should be used to augment and enhance current syndromic surveillance systems to provide earlier warning of a pandemic or terrorist incident.

## Intelligence Sensors

One possible expanded role for EMS personnel is in the area of acting as intelligence sensors. With some focused training, EMS personnel could become aware of the tactics and tools of terrorists and learn when it would be appropriate to report suspicious activities to the proper authorities.[5] EMS personnel are uniquely qualified to fill this function because EMS personnel see many things that no one else will see in the course of their duties. EMS personnel respond into all types of situations where potential terrorists, experiencing an emergency, may not have had the time to cover or conceal their activities. EMS personnel may be the only individuals that are exposed to these potential threats before they occur. As Petrie observes:

> We go into all locations with short notice and without the baggage that law enforcement has, we are trained observers, we go everywhere, apartments, houses, we are not viewed as a threat and we have the ability to observe things that are going on.[6]

This type of reporting is not without controversy. Some in EMS would say that this is a job for law enforcement and has no place in EMS. However all EMS personnel are now required to report other suspected issues such as child or elder abuse. Possible terrorist activities could fall into a similar reporting paradigm for EMS. In addition, many EMS agencies are very much involved in prevention efforts. EMS in many areas provides training and education in bike safety, pool safety, and car seats. Reporting potential terrorist acts could fall into a prevention of injury category and could be considered a positive contribution of EMS personnel to the homeland security effort, to the nation, and to local communities. Reporting specific suspicious activities related to homeland security could greatly enhance response to a potential threat and provide EMS an opportunity to participate as full partner in homeland security activities.

## Analysis of Medical Data and linkage to the Clinical Community

EMS personnel could identify the clinical and operational significance of certain information in fusion centers and serve as a link to the clinical community within a jurisdiction. This is a critical component of force protection.

A qualified paramedic, who is trained as a medical intelligence analyst, could answer the following questions using terminology easily understood by first responders and public safety personnel, and distribute that information in a medical intelligence bulletin:

- What is the potential impact to fire, law, correctional and EMS personnel if many expats from a country with high malaria risk travel to that country for the holidays then return to our jurisdiction?
- Do first responders need to take any precautions in response to a large outbreak of Salmonella or Influenza in the community?
- What do first responders need to know to provide proper treatment to patients taking a new ecstasy-based pharmaceutical?

Reporting suspicious activities by EMS requires a proper reporting mechanism be in place where EMS reports would be taken seriously and synthesized into useable intelligence. The most logical place for this to take place is the local fusion center. There are over seventy-five fusion centers across the nation and their mission is to collect and analyze intelligence data from all sources and then to provide reports back to local, state, and federal agencies that would help mitigate terrorist or naturally occurring disaster events. By contributing to this collective effort, EMS has the opportunity to exchange valuable information with field personnel about possible threats and danger where they work.[7] This exchange of information provides a chance to work more closely with a variety of partners in the community and that collaboration alone can have positive effects for local EMS agencies. Petrie states: "Just as you can't ask a paramedic to interpret the law, you can't ask a law enforcement officer to interpret medical information."[8] Medical professionals should analyze data and trained personnel could determine how to not violate local, state, and federal confidentiality laws. Local EMS providers should have representation on the local boards of fusion centers to facilitate this exchange of data and ideas. Collaboration and cooperation could lead to more responsibilities and the identification of logical ways to increase EMS synergy with the other agencies in their region.

## EMS as the Multi-Casualty Incident/ Event Planning Lead Agency

EMS personnel are the experts when it comes to pre-hospital care. They understand their populations, normal response areas, regions, hospitals, and capabilities. They currently service all of the medical institutions within their jurisdictions and understand the flow of patients in normal and surge situations. With this knowledge they are uniquely situated to be the lead planning agency for mass casualty incidents such as terrorist attacks or natural disasters. These EMS agencies understand current capabilities, how those capabilities will

be affected when an overload occurs, and where to expect help within their regions. Gap analysis can be completed and exercised to determine where weaknesses exist and where patients are most at risk during a catastrophic event.

EMS personnel work daily in treatment and distribution of patient loads and specific patient illness and trauma triage. Basic training of EMS personnel includes discussions and practice of appropriate destination analysis and proper treatment to maximize positive patient outcomes. Since EMS provides this service on a daily basis, EMS is the logical lead for mass casualty incident and logistical planning.

## Development of EMS-Based Response Teams

The Department of Homeland Security (DHS), through the Federal Emergency Management Agency (FEMA), should develop models of EMS based response teams that can respond to manmade and terrorist disasters in a comprehensive manner across all jurisdictions and boundaries. These teams should work first within local jurisdictions, then in regions, then in states, and finally across state lines to meet the needs by expanding as needed based on event type and what expertise is needed.

EMS strike teams are typically five ambulances with a strike team leader. Multiple strike teams can constitute an EMS task force, which provides various support components to keep the teams independent and mobile in any environment. This model can be adapted and molded to meet the need of any specialized situation. This model of response could well be used within law enforcement teams to include EMS in the makeup to strengthen a response in an unstable situation that has multiple medical components. The combination of medical expertise and security could quickly and definitively respond to and meet the needs of victims while keeping all responders safe and law enforcement healthy. EMS components in all types of search and rescue are necessary since it is never known when treatment and transport of victims will be demanded. EMS involvement in all types of responding teams in disasters provides not only direct medical care for victims, but also a peace of mind for responders that are outside of normal, conventional environments and are exposed to a variety of hazardous conditions. Immediate medical care, treatment, health safety, and more are critical to all disaster missions and EMS is the conduit to including all of those components in a response team.

With proper networking, all of these response teams could form a strong system of local, regional, statewide, and national response that is expandable as needed and could easily be collapsed as the disaster is controlled. Use of Incident Command and other common principles combined with a common training model across jurisdictions could provide the needed coordination protocols to make response seamless. DHS through FEMA is the logical agency to coordinate nationwide implementation of this neighbor-helping-neighbor model using current EMS resources.

## EMS Role in Data Management and Analysis

One last area of EMS participation is with its data.[9] EMS data received from dispatch, run reports, and directly from field personnel could provide invaluable insight into a developing terrorist attack or pandemic event.[10] EMS data could shed light on a trend that indicates a needed action to mitigate a circumstance to reduce death or injury. EMS collects data that no other agency does. This data is unique and can be applied to other analysis to create a clearer picture of a possible developing event.

An example would be looking for a series of symptoms that include fever, nausea, and vomiting at unusual levels. If an EMS system's normal level of these symptoms are five a day and suddenly there have been ten sets of these symptoms in the last hour, this could be an indicator of unusual activity.[11]. Computer software is available that can sit in the background and monitor EMS data to provide a syndromic surveillance solution that would give an early warning of possible threats. This software could be preset to monitor specific data points linked to a biological or chemical attack or a naturally occurring disease process.[12] Each

individual EMS crew working a regular shift might not see a trend in the making; however the software might see a trend developing before any individual would notice. Many parameters such as response times or patient drop times could be monitored, but the ones most valuable to homeland security efforts would be those related to the types of calls EMS is dispatched to and the symptoms patients are experiencing.[13] Data would need to be collected in aggregate form so that individual protected patient information is not disclosed. All aspects of patient privacy must be addressed.[14]

### New EMS Roles in Disaster Recovery

After the initial phase of a disaster occurs, many times the function of EMS response diminishes and EMS personnel have few roles in recovery. EMS agencies should look for new ways to integrate into recovery efforts and improve the overall quality of life in their communities.[15] One possible area of involvement would be damage assessment. Damage assessment teams would benefit from paramedic involvement in many ways. First, if patients are discovered during assessment, treatment can begin immediately. Next, EMS personnel are trained and many are experienced at some level of safety and hazard assessment. With a little more training, this knowledge and experience could supply valuable insights into potential hazards and possible solutions for health related issues. Other roles in recovery should also be explored such as providing a variety of health services in the community, from wound care to immunizations post disaster. The skills of EMS personnel are many and ways to utilize those skills appropriately should be explored. EMS personnel could help their local communities recover faster from a disaster and provide specific help in the field where no other help exists.

## CONCLUSION

EMS has demonstrated its ability to expand its role in many ways in healthcare delivery. Homeland security is another area where EMS must be involved fully. EMS is one of the three main response agencies notified when 911 is called, along with fire and law enforcement. In order for EMS to be recognized as a valuable partner in homeland security, EMS needs to find creative ways to provide real services to the homeland security community that make a difference and provide value. With a workforce of nearly 900,000, EMS has trained, professional personnel in all corners of the nation and with a little more training, a little more equipment, and a positive attitude, EMS stands to improve homeland security response and improve the quality of life of citizens served. EMS is the logical choice to perform these homeland security functions and to perform them well. Accepting expanded roles in homeland security could increase needed funding and provide more respect for a discipline that is well deserving and ready to meet the challenge of a changing world.

## ABOUT THE AUTHOR

***Mac Kemp*** *is deputy chief of operations at Leon County EMS and recently graduated from the Masters of Security Studies Program at the Naval Post-Graduate School, Center for Homeland Defense and Security in Monterrey, CA. He also holds a Masters of Education from Florida State University. He can be reached at kempm@comcast.net.*

## NOTES

1. Leeanna Mims, "Improving Emergency Medical Services (EMS) in the United States through Improved and Centralized Federal Coordination" (master's thesis, Naval Postgraduate School, March 2011).

2. Lauren Simon Ostrow, "The Controversy Over EMS, Homeland Security and the Feds," *Best Practices in Emergency Services* 8, no. 6 (2005): 61-63; Joseph A Barbers, Anthony G. Macintyre, and Craig A. DeAtley, *Ambulance to Nowhere: America's Critical Shortfall in Medical Preparedness for Catastrophic Terrorism* (Washington, DC: George Washington University John F. Kennedy School of government, 2001).

3. Michael Petrie, "The Use of EMS Personnel as Intelligence Sensors: Critical Issues and Recommended Practices," *Homeland Security Affairs Journal* 3, no. 3 (September 2007).

4. Federal Interagency Committee on Emergency Medical Services, *2011 National EMS Assessment,* DOT HS 811 723 (Washington, DC: U.S. Department of Transportation, National Highway Traffic Safety Administration, 2012), 1, www.ems.gov

5. Thomas J. Richardson, "Identifying Best Practices in the Dissimenation of Intelligence to First Responders in the Fire and Ems Services" (master's thesis, Naval Postgraduate School, September 2010).

6. Petrie, "EMS Personnel as Intelligence Sensors."

7. James F. Morrissey, "Strategies for the Integration of Medical and Health Representation within Law Enforcement Intelligence Fusion Centers" (master's thesis, Naval Postgraduate School, March 2007).

8. Petrie, "EMS Personnel as Intelligence Sensors."

9. Clay N. Mann, "Introduction to the National Emergency Medical Services Information System (NEMSIS) and its Potential use in Syndromic Surveillance" (Atlanta, GA, International Society for Disease Surveillance, January 31, 2012, 2012).

10. Jonathan Busko, "EMS and Medical Surveillance," EMSWorld.com, February 1, 2007, http://www.emsworld.com/article/10322103/ems-and-medical-surveillance.

11. Kristin Broome Uhde, "Bioterrorism Syndromic Surveillance: A Dual-use Approach with Direct Application to the Detection of Infectious Disease Outbreaks" (PhD Dss., University of South Florida, 2003).

12. Matthew Raymond Groenewold, "Reliability and Validity of EMS Dispatch Code-Based Categorization of Emergency Patients for Syndromic Surveillance," (PhD diss., University of Louisville, March 2008).

13. D. Fishbein, et al., "Public Health Surveillance Using Emergency Medical Service Logs- U.S.-Mexico Land Border, El Paso, Texas, 2009," *MMWR: Morbidity & Mortality Weekly Report* 59, no. 21 (June 2010): 649.

14. Khaled El Emam et al., "A Secure Protocol for Protecting the Identity of Providers when Disclosing Data for Disease Surveillance," *Journal of the American Medical Informatics Association* 18, no. 3 (April 2011): 212-217.

15. Gregory Bennett, *Cross-Training for First Responders* (Boca Raton, FL: Taylor and Francis, 2010).

# Leveraging Emergency Notification Alerts

Michael Leiva

## ABSTRACT

*This essay argues for the importance of either creating a new alert system or changing the criteria of the current Emergency Alert System. Such an alert system is critical in assisting emergency managers and law enforcement personnel with communicating safety and security concerns. To use the current system, local and state government officials must complete the Integrated Public Alert and Warning System (PAWS) process.*

## INTRODUCTION

The Department of Homeland Security (DHS) and other federal organizations such as the National Weather Service (NWS) have access cell phone alert system. But this access requires local and state municipalities to become accredited by the Federal Emergency Management Agency (FEMA) before they can be authorized to use the system. Due to the delay in the accreditation process, local/state governments and even education centers have started or created their own emergency alert systems with mobile and internet capabilities. This creates a redundant system, which is can be beneficial but can also lead to information fratricide by reporting inconsistencies or over-reporting. This redundant system also has drawbacks; for example, subscribers may use a particular service from a school or town, but an adjacent school or town reports an incident using a different service. In the end, the subscriber concerned does not receive a notification. For a multitude of reasons, local and state government officials must be accredited and have access to transmit and notify citizens on the national alert system. This essay discusses the background and creation of the national alert system, the Integrated Public Alert and Warning System (IPAWS), and the need for local and state government officials and emergency managers to access and transmit on the IPAWS.

## Background and Creation of the National Alert System

The National Weather Service (NWS) frequently sends out Wireless Emergency Alerts (WEA) about "weather watches, warnings and advisories from both the Common Alerting Protocol (CAP) and Atom Syndication Format (ATOM) through the Emergency Alert System (EAS)."[1] According to the NWS these alerts can be "used to launch Internet messages, trigger alerting systems, feed mobile device (e.g., cell phone/smart phone and tablet) applications, news feeds, television text captions, highway sign messages, and synthesized voice over automated telephone calls or radio broadcasts."[2] They can also be specifically targeted to mobile devices operating in a certain geographical location or receiving signals from certain cell towers.

Rather than build a new communication platforms, the Department of Homeland Security (DHS) leveraged and improve the existing National Weather Service (NWS) system for emergency management purposes. On June 26, 2006, Executive Order 13407 authorized the Secretary of Homeland Security to:

> Establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system to enable interoperability and the secure delivery of coordinated messages to the American people through as many communication pathways as practicable, taking account of Federal Communications Commission rules as provided by law.[3]

This Executive Order created the Integrated Public Alert and Warning System (IPAWS) program, which enables the Federal Emergency Management Agency (FEMA) DHS to alert and warn US citizens, protecting property and preserving life through the Federal Communications Commission (FCC).

## The Integrated Public Alert and Warning System (IPAWS)

With the recent increase in violent crimes inflicting mass casualties or panic, destructive weather incidents, or other hazardous emergencies, disseminating timely and accurate information must be the responsibility of local government officials. Currently, both local and state government organizations must be authenticated by FEMA before they can use the Integrated Public Alert and Warning System (IPAWS) or transmit using its software. "As of January 2013, 93 public-alerting authorities, 18 including those in at least 35 states, have gone through the necessary authentication steps with FEMA to use IPAWS and an additional 110 alerting authorities have applications in process."[4]

During the Sandy Hook Elementary School Shooting and the Boston Marathon Bombing tragedies, local government, law enforcement and emergency management officials were able to use IPAWS to send out some critical public information. In both instances, alerts ranged from a couple of minutes to almost two hours.[5] During the Waldo Canyon Wildfire, Colorado, in June 2012, approximately 50,000 out of a potential 118,000 residents signed up for the local emergency notification system within three days in order to receive timely updated information.[6]

In order to better serve and protect the public, emergency management at the local and state government level needs to disseminate timely critical information to a specific area. Integrating the IPAWS alert system assist with all emergencies in which emergency managers need to inform the public of safety concerns and security measures or possibly request assistance in solving a crime.

## Reason for IPAWS at the Local Government Level

Emergency response to disasters will always be further complicated because of communication issues. Communications during an emergency can lack focus or contain little to no information; or they can provide directions to public safety locations, create a citizen reporting hotline, and/or inform concerned or affected citizens of a hospital(s) patient registry. The goal of government officials, during emergency disasters, should be to avoid disseminating inaccurate information. The reason to avoid this is simple: misinformation will be repeated and cause more confusion then assistance.

Emergency management personnel and local government officials must be able to utilize IPAWS or develop a similar system with same capabilities in order to disseminate critical information that will save lives or protect government/personal property. There are three things local government must do to make IPAWS more effective: (1) local government and emergency management departments need to begin and complete the IPAWS accreditation process through FEMA; (2) local citizens must be more proactive and subscribe to and sign-up for the local emergency alert notification system; and (3) FEMA must provide a clear definition, with examples, for all emergency alerts, that allows local governments and emergency managers through local legislation to add specific regional emergency threats that may not be relevant in other areas.

## IPAWS Accreditation Process

The four-step process to become an IPAWS approved alerting authority includes: using an IPAWS compatible software system to send the alerts, completing a memorandum of agreement with the FEMA for use of IPAWS system, applying to FEMA to send public alerting permission, and completing Internet-based IPAWS training from FEMA's Emergency Management Institute website.

According to a GAO report, one of the main obstacles to government officials using the IPAWS system is lack of training. In this report, emergency managers across the nation

were surveyed and responded that they lacked training, specifically how to "properly craft and initiate a message… as well as make the system more user-friendly."[7] Since this GAO Report's findings were released nine public and private Universities, nineteen ADA/People with Access and Functional Needs Organizations, and several other government authorities have become IPAWS accredited.[8] Making the IPAWS system more user-friendly and providing operator training for current and future users will facilitate the ability of emergency managers and government officials to effectively alert the public.

## Becoming Proactive

One of the nation's first pioneers of the "subscribed" alert messaging system was Virginia Tech University. After the campus shooting on April 16, 2007 that resulted in thirty-two dead and seventeen wounded, the Governor's Office ordered a report be made. In the *Mass Shootings at Virginia Tech Report, Key Findings Section*, four of the twenty-one findings discuss alert communications and notifications.[9] Virginia Tech has since created VT Alerts and the university Office of Emergency Management has created VTGemini; both systems are multi-modal alerts that send messages to inform subscribers of emergencies and recommend a course of action to follow.[10] VT Alerts and other similar systems are proactive approaches but do not account for people who choose not to subscribe or guest and visitors who are in the area but have not subscribed for these alerts. In response to tragedies and emergencies like the Virginia Tech Massacre, many businesses, schools, organizations, and city councils created their own emergency alert notification systems. Some of these organizations require their employees, students, or parents to subscribe to these notifications; others are voluntary. This methodology, although it may not require the individual to subscribe for the notification system, is still proactive as it informs the individual of the alert system and allows them to subscribe or not subscribe for the service.

## Emergency Disaster Defined

FEMA currently has over fifty definitions for "disaster." Although this seems inconsequential, the reality is that organizations, government officials, and emergency managers throughout the United States react differently during disasters. Without having a standard definition for "disaster," emergency managers or other government officials are inhibited in providing support and confronting the disaster. FEMA's basic definition for disaster is "an occurrence that has resulted in property damage, deaths, and/or injuries to a community."[11] The World Health Organization (WHO) defines a disaster as "serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources" and an emergency as "imposed by somebody in authority, who, at a certain moment, will also lift it. Thus, it is usually defined in time and space, it requires threshold values to be recognized, and it implies rules of engagement and an exit strategy."[12] All emergency disasters need these two critical pieces: quantification of loss of life, equipment, and property which exceed the local level ability to respond to it, and the appointment of somebody who has the authority to mitigate, react, and respond to a disaster for a finite period of time.

With this understanding, emergency managers or government officials can place restrictions on emergency alerts that are sent to the public. Furthermore emergency managers, with the help of FEMA, can better define events that would require an emergency alert.

## CONCLUSION

In order to leverage existing emergency notification alerts or Integrated Public Alert and Warning System (IPAWS), on the national level through FEMA, government officials and emergency managers need to become more proactive, seek for their organization or agency to become IPAWS accredited, and establish a standard definition of an emergency disaster with examples.

## ABOUT THE AUTHORS

***Michael Leiva**, is an Active Duty Army Major with over ten years of service. He has deployed several times, most recently to a military transition team in Tikrit, Iraq. Major Leiva is a graduate Tulane University's graduate Homeland Security Program and is currently working on his Certified Emergency Manager accreditation packet.*

## NOTES

1. *NWS Public Alerts in XML/CAP and ATOM Formats.* National Oceanic and Atmospheric Administration's National Weather Service, July 29, 2013 http://alerts.weather.gov/

2. Ibid., 2.

3. Government Accounting Office. *Presidential Documents; Executive Order 13407 Public Alert and Warning System*. [71] *Federal Register* (Washington, DC: GPO, 2006).

4. Government Accounting Office. *EMERGENCY ALERTING: Capabilities Have Improved, but Additional Guidance and Testing Are Needed* (Washington, DC: GPO, 2013).

5. Gary A. Klug, *Waldo Canyon Fire ANALYSIS OF EMERGENCY NOTIFICATION SYSTEM UTILIZED BY THE EL PASO/TELLER COUNTIES E911 AUTHORITY DURING THE WALDO CANYON FIRE, JUNE 23, 2012 TO JUNE 29, 2012* (Colorado: 2013).

6. Virginia Tech Review Panel. *Mass Shootings at Virginia Tech Report of the Review Panel*, http://www.governor.virginia.gov/TempContent/techPanelReport-docs/4%20SUMMARY%20OF%20KEY%20FINDINGS.pdf

7. "VT Alerts," *Virginia Polytechnic Institute and State University*, http://www.alerts.vt.edu/index.html

8. Government Accounting Office. *IPAWS Partner Organizations* (Washington, DC: Federal Emergency Management Agency, May 2013), http://www.fema.gov/media-library-data/20130726-1915-25045-7294/ipaws_partner_organizations_may2013.pdf

9. Government Accounting Office. *Emergency Preparedness: Improved Planning and Coordination Necessary for Modernization and Integration of Public Alert and Warning System* (Washington, D.C: GPO, 2009).

10. Government Accounting Office. *IPAWS Partner Organizations*.

11. Government Accounting Office. SLG 101: *Guide for All-Hazard Emergency Operations Planning* (Washington, D.C: GPO, 1996), http://www.fema.gov/pdf/plan/glo.pdf

12. Ibid.

# James Phelps, Jeff Dailey, and Monica Koenigsberg, *Border Security*

(Durham, NC: Carolina Academic Press, 2014)

Reviewed by Robert J. Bunker

The new work *Border Security* written by James R. Phelps, Jeff Dailey, and Monica Koenigsberg is close to four hundred pages in length and can be considered the definitive tome on the topic as it relates to US border security perceptions, practices, and issues. The work is both comprehensive in scope and holistic in its approach. Underlying themes to the book are that border security is in many ways timeless (e.g., the Great Wall of China and Hadrian's Wall), with past states and peoples coping with similar issues that we have today, that is, allowing those in who should be let into a state and keeping others out who somehow threaten a state and its people. Further, border security within the work is viewed more within the context of a long term defense-in-depth rather than just as a linear defense.[1] Also, the work rightfully argues that short-term border security fixes rarely work as planned and may actually make a bad situation even worse.

The authors, all faculty PhDs in various criminal justice, border and homeland security, and security studies programs at Angelo State University, San Angelo, Texas bring a wealth of experience to this work. Phelps, who also is retired US Navy, penned nearly half of the chapters. Dailey, who also has a military intelligence background with the NSA, Navy, and Air Force, and Koenigsberg, with her policing and prison officer background, also bring practitioner expertise to their contributions. This combination of academics with real world experience is very valuable in an applied academic work in the security field.

The book is organized into three parts: I. Defining Borders (ch.1-5); II. Border Security and Transnational Crime (ch. 6-9); and III. U.S. Border Security Today (ch. 10-12) with the following chapter subdivisions: (1) Barriers, Boundaries, and Borders; (2) Border Security in History; (3) Border Security Agency Operations; (4) Physical Border Security; (5) Maritime Border Security; (6) Trafficking: Contraband, Smuggling and the Law; (7) People Movers: Human Trafficking and Population Migrations; (8) Borders, Economic Interdependence, and Internet Crime; (9) Transportation Security; (10) The U.S.-Mexico Border; (11) The U.S.-Canadian Border; and (12) The Future of Borders and Boundaries in the Modern World. Each chapter has accompanying endnotes. Front sections include a foreword, acknowledgements, and author biographies. A detailed index is contained in the back of the book.

The strengths of the work are that it analyzes today's border security issues from a solid historical basis. No partisan politics were detected in the work and so the writing does not appear to be politically motivated or skewed. The work covers the myriad of border security issues as individual and intertwined problems, which allows the reader an integrative perspective on the dynamics of border security. Still, a few weaknesses are evident. As a textbook, it would be appropriate to have some sort of key terms listing at the beginning of chapters or within the text. Also missing are review and discussion questions at the ends of the chapters. These omissions have been noted by the authors and will be added in later editions of the textbook. In the meantime, key terms and review and discussion questions will be provided in the forthcoming instructor's manual. This reviewer very much enjoyed reading the various chapters but at times – given the clinical nature of the text and the analytical

writing style taken – certain sections were not easy to comprehend and required a second reading to better understand the concepts and examples provided.

The contribution of the work to this field of study is that it provides a first look at border security as an essential component of homeland security. The work is written from an academic perspective and not from that of a first person storytelling narrative as so many works on this topic have been in the past; see for example, Lee Morgan's *The Reapers Line* (Rio Nuevo 2006). Except for the contemporary work *U.S. Border Security: A Reference Handbook* by Judith Warner (ABC-Clio 2010) – interestingly enough also an academic from Texas – there are no other textbooks on border security.[2] The Warner text was specifically written as a reference resource and offers very useful reference material with many chronologies, biographical sketches, data and documents, directories, and other resources; this reviewer strongly suggests it as a supporting text in courses on the topic of border security. Of the two works, *Border Security* has the obvious edge, in that it was actually developed as a college textbook for teaching purposes. As a result, this new work will set the standard for all subsequent authors approaching this subject with a textbook in mind.

In summation, *Border Security* is a comprehensive and in-depth work on border – and homeland – security with excellent utility for both undergraduate and graduate level courses. It establishes a baseline for more focused discussions on a wide range of important topics intimately tied to the international problem of homeland security. Further, *Border Security* provides detailed coverage of both historical and contemporary issues in a clear and concise manner for the university student and should be considered essential reading for anyone wanting to participate in border security discussions. Given the size and scope of the text, it is fairly priced at $60.00.

## ABOUT THE AUTHOR

***Dr. Robert J. Bunker*** *is a distinguished visiting professor and Minerva Chair at the Strategic Studies Institute, U.S. Army War College. He is also adjunct faculty, Division of Politics and Economics, Claremont Graduate University. Disclosure: The author provided a back cover endorsement of the work and was also a galley reviewer. All views are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the United States government.*

## NOTES

1. The reviewer could not agree more with this viewpoint. See Robert J. Bunker, "U.S. border security spending: Too much, too late?" Baker Institute Blog. *Houston Chronicle*, July 30, 2013, http://blog.chron.com/bakerblog/2013/07/u-s-border-security-spending-too-much-too-late/.

2. The work by Andrew Staniforth and Police National Legal Database (PNLD), *Blackstone's Handbook of Ports & Border Security Paperback* (Oxford 2013) also has a lot of merit but is UK focused and far more applied in nature. It is meant for UK police officers engaging in port and border security duties and as a result is more of a training, rather than an educational, resource.

# *The Siege of Mecca* by Yaroslav Trofimov

(New York: Doubleday, 2007)
Reviewed by Matthew Magolan

The terrorist siege of the Grand Mosque at Mecca in Saudi Arabia between November 20 and December 4, 1979 has been relegated to a footnote in the American historical consciousness. The siege was sandwiched between the beginning of both the U.S. Iranian Embassy hostage crisis, which began on November 4, 1979, and the Soviet invasion of Afghanistan on December 24th of the same year. The details surrounding the unprecedented attack on Islam's holiest mosque reveal information that foreshadows the deadly brand of global terrorism which rose from the fundamentalist *Wahhabi Sunni* Islamic tradition of Saudi Arabia and threatens the United States to this day. *The Siege of Mecca* by Yaroslav Trofimov is a well-researched and insightful account of the extraordinary events in which over 200 Islamic militants took the holiest site in the Muslim faith by the force of arms.

The *Fedayeen* style assault on Mecca served as a rough blueprint for the Mumbai attack in November 2008, the Mehran Naval air station attack in Pakistan during May 2011, the Intercontinental Hotel attack in Afghanistan in June 2011, the attack by 100 militants on a police station in Pakistan in October 2012, and the attack on the Westgate Mall in Kenya in September 2013. It seems that old has become new again and analysts indicate that small unit-small arms type attacks will be among the most preferred terrorist attack methods of the future.[1] Unlike other countries where elite military units respond to these attacks, American police officers will be tasked with an effective initial response to a small unit-small arms attack in the United States. *The Siege of Mecca* is an excellent account of the terrorist uprising at Mecca, which presents valuable lessons for both American law enforcement and the greater homeland security community.

Trofimov has covered Saudi Arabia for the *Wall Street Journal* since 1999 and his ability to explain the greater context of the siege is evident. The author effortlessly weaves history, politics, religion, sociology and the event itself into a cohesive narrative that reads more like an action thriller than the genuine work of investigative journalism that it is. Juhayman al Uteybi, a charismatic preacher in *madrassas* (Islamic schools) in Saudi Arabia, was the mastermind behind the plot. Juhayman began teaching in state sponsored madrassas spreading the doctrine of Wahhabi Sunni Islam, but became disenfranchised when the western-influenced modernization of the Kingdom of Saudi Arabia was contradictory to the spare and puritanical teachings of this tradition. Juhayman first attempts to enlist his own teachers from the *Ulema* (a body of clerics who direct the spiritual and moral compass of Saudi Arabia) to publicly recognize the hypocrisy of the Royal Family. When he is rebuffed by the Ulema and their realpolitik attitude toward the Royal Family, Juhayman believes that they too are hypocrites and sets off on his violent path.

The narrative of Juhayman's descent into violent anti-establishment Islamic radicalism reads similarly to that of domestic serial bomber Eric Rudolph's downward spiral into violent anti-establishment Army of God Christian radicalism.[2] A poignant point, for me, was that radicalism is radicalism no matter which Book it comes from. The warning signs and mentality are doppelgänger profiles on opposite sides of the same coin. The madrassas in Saudi Arabia where Juhayman taught were fertile grounds for him to recruit devout acolytes. Young men raised in the Wahhabi tradition and conscious of the obvious incongruity between the Wahhabi lip service of the Royal Family with the cover of the Ulema and the reality of their actions. From these committed madrassa students, many of whom had been tactically trained in the Saudi

Arabian National Guard, Juhayman built his Fedayeen army.

The book tackles the quandary of the duality of the Saudi Arabian state: on one hand, a staunch political ally of the United States and much of the modern West, but, on the other hand, the premier worldwide conduit of radical Wahhabi Sunni Islamic beliefs which call for the destruction of the non-Sunni world. Trofimov paints a vivid portrait of the history of Saudi Arabia. Beginning with nomadic Bedouin origins in the *Nejd*, he follows the rise and fall of conquerors, kings and scoundrels, ending, finally, with the rise of al Saud and the modern Kingdom of Saudi Arabia. The Sunni populace of Saudi Arabia is torn between allegiance to the Al Saud family and the Quran as interpreted by the ultra-fundamentalist Ulema. Trofimov connects the dots of this complex history in a descriptive narrative.

Much of Juhayman's anti-Royal Family sentiment was initially stoked by the Ulema who often questioned, but never overtly challenged, the Saudi Royal Family. In an interesting plot twist of the siege, the Saudi Royals must bargain with the Ulema to gain a *fatwa* (ruling) that will allow the Saudi government to attack the terrorists in Mecca, even though it is forbidden to carry weapons or fight in Mecca according to the *hadith* (sayings of the Prophet). The end result of the need for the *fatwa* was that the Ulema used its leverage to exact a promise from the Saudi government to pay billions of petro-dollars toward more madrassas. These new madrassas would spread even more of the same fiery Wahhabi fundamentalist Islamic rhetoric that created the siege in the first place: an ironic state of affairs that would create far-reaching ramifications felt to this very day.

Juhayman believed he had the full force of the hadith behind him. Juhayman and his men believed that one of his men, Mohammad Abdullah al Quraysh, was the *Mahdi*, an invincible Islamic redeemer who, according to Islamic lore, will lead Muslins to an ideal Islamic world after an apocalyptic clash with the forces of evil (including all non-believers). This apocalyptic belief was the final push for Juhayman and his men to take over the mosque. The House of al Saud had to re-take the mosque to save face among the Islamic world at large.

The Saudi government forces were handed defeat after defeat in battle after battle with Juhayman's small army, who were motivated by religious fervor, tactically trained and in defensive positions throughout the fortress-like mosque. Only when the armored brigades of the Saudi Army used M113 armored personnel carriers, artillery, and TOW missiles did the Saudi government forces gain even a foothold in the courtyard on the ground level of the Grand Mosque. This was only after more than a week of heavy fighting. Juhayman and his men then retreated to the *Qaboo*, a labyrinthine maze of narrow chambers and corridors underneath the mosque where the terrorists would make their final stand.

The Saudi forces had poor intelligence and inaccurate blueprints for the *Qaboo*. Juhayman's men, many of whom had intimate personal knowledge of the layout of the *Qaboo* from their religious observances at the mosque, made the counter-assault a deadly mission. Even as the Saudi government tried to tell the world that the terrorists had been defeated, the fighting raged on. In near desperation, the Saudis turned secretly to the expertise of the elite French counter-terrorism unit *Group d'Intervention de la Gendarmerie Nationale* (GIGN). Interestingly, Trofimov explains numerous times in his narrative that the Saudis failed to recognize the siege as a military problem, but then seemingly misses the fact that the GIGN is a special paramilitary police force similar to the FBI Hostage Rescue Team: a small misinterpretation of the grey world of tier I counter-terrorism units in an otherwise excellent narrative.

After two weeks of outright warfare, three GIGN Commandos, acting only in an advisory role, finally gave the Saudi forces the tools, tactics, and training needed to overcome Juhayman's men. The casualties on both sides were enormous. Saudi government sources place the rebel casualties at 117 dead and 150 captured. The Saudi government also claims that 127 soldiers were killed along with 450 wounded. Western intelligence estimates place

all of the dead at over 1,000. The true numbers will likely never be known.

Trofimov conducted his research without the consent of the Saudi government, which still keeps the information from the siege classified. The Saudis have even kept most of the information about the siege from western intelligence agencies. The ironclad grip the Saudi government maintains on any information related to the event makes *The Siege of Mecca* an even more impressive journalistic accomplishment.

Trofimov describes the ripples of violence spreading throughout the region in this tumultuous time. The US embassy in Islamabad, Pakistan was burned to the ground when the Iranians wrongly blamed the siege of Mecca on US and Israeli paratroopers. The US Embassy in Tripoli, Libya was overrun by protestors. All over the Muslim world icons of the West were burned, destroyed, or looted by misinformed people believing that Western forces were responsible for the siege at Mecca. Trofimov makes an airtight case that the siege at Mecca was a catalyzing event for widespread contemporaneous unrest throughout the Middle East. The book finally connects the events of Mecca with the modern fundamentalist Islamic threats faced by the United States and our allies. The small multi-national army Juhayman assembled was, in many ways, a blueprint for Al Qaeda. Hindsight is always 20/20, but Trofimov has found a lens that focuses seemingly distant historical events into a clear picture of how those events directly influence the present and future of international terrorism and counterterrorism.

Although it is unlikely that American law enforcement officers will see a small unit-small arms assault comprised of over 200 attackers on American soil, it is exceedingly possible that a smaller small unit-small arms terrorist attack will occur in the United States within the next ten years. Small arms attacks are among the easiest types of attacks to perpetrate in our post 9/11 society. Small arms are readily available in the United States and, with the right connections and funding, across our border to the south.[3] Instability due to the narco-war in Mexico creates a permissive environment for the possible infiltration of individuals wishing to inflict harm upon the American people.[4] And with the killing of Osama Bin Laden, our fundamentalist Islamic enemies have a new motivation to find novel ways to attack the United States,[5] sowing the seeds of terror anew.

Our enemies have a long memory and infinite patience. *The Siege of Mecca* by Yaroslav Trofimov gives American law enforcement a unique view into the roots of modern fundamentalist Islamic terrorism within an important historical context. A context that directly influences our current and future homeland defense challenges with an adaptive and unwavering enemy.

## ABOUT THE AUTHOR

***Matthew Magolan*** *is a police officer with the City of Madison Police Department in Madison, Wisconsin. He is a member of the Special Events Team and works with the MPD Emergency Preparedness Committee. In addition to his duties as a patrol officer, he conducts contingency planning and site security surveys for major events that take place in the City of Madison. He has developed practical active shooter training for community partners. Matthew Magolan can be reached at mattmagolan@yahoo.com.*

## NOTES

1. Angel Rabasa, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak and Ashley J. Tellis, "The Lessons of Mumbai," Occasional Paper, RAND Corporation (2009).

2. "Eric Rudolph's Manifesto," Associated Press, April 18, 2005, http://archive.decaturdaily.com/decaturdaily/news/050418/manifesto.shtml.

3. Ioan Grillo, "Mexico's Drug Lords Ramp up Their Arsenals with RPGs," Time World, October 25, 2012, http://world.time.com/2012/10/25/mexicos-drug-lords-ramp-up-their-arsenals-with-rpgs/#ixzz2AdtkCXEG

4. Deroy Murdock, "The Southern Border: Our Welcome Mat for Terrorists," National Review Online, April 25, 2013, http://www.nationalreview.com/article/346591/southern-border-our-welcome-mat-terrorists.

5. "Lashkar-e-Taiba Surpasses al-Qaeda as the Biggest Terrorist Threat from South Asia, Says TRAC," Terrorism Research & Analysis Consortium (TRAC), posted October 16, 2012, http://www.prweb.com/releases/2012/10/prweb10015059.htm.